User Manual
KVM IP Console Module Card
DIP-101

Rev. 1.0
2010.05.31

Table of Contents

1 Introduction

The IP Console Module is a cost-effective solution to enhance the management ability of KVM switches. It allows you to manage servers from anywhere via an IP without upgrading your KVM equipments. By just sliding the module into KVM Switch, you can easily upgrade your KVM switches to IP level.

1.1 Features

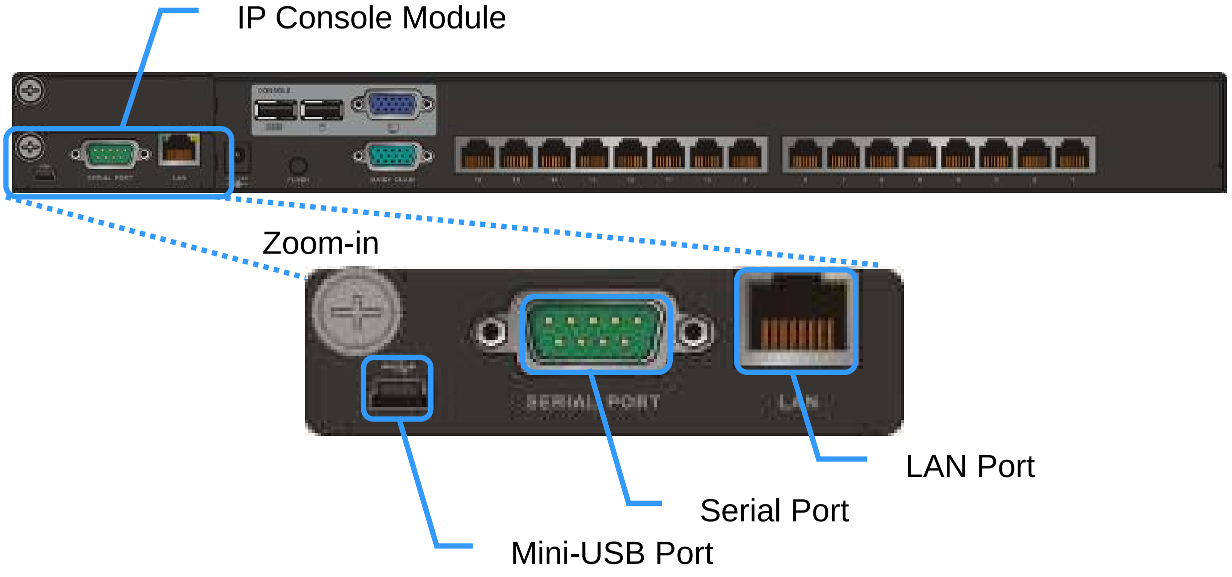
- Manage servers around the world.
- KVM (keyboard, video, and mouse) access over IP
- Full control under any OS, in BIOS mode, during boot, at Blue Screens
- No additional software necessary on servers
- 256 bit SSL encryption of all transmitted data and Certificate management
- High-performance mouse tracking and synchronization
- Automatic adjustment of data rate to transmission line
- Remote mass storage control
- Can be controlled over all java-enabled Browsers
- Firmware update via web interface
- Port to connect a user console for direct analogous access to KVM switch

1.2 Package Contents

- 1 x KVM IP Module Card
- 1 x CD (Software & Manual)
- 1 x Desiccant

Contact your reseller if any of above items are missing or damaged.

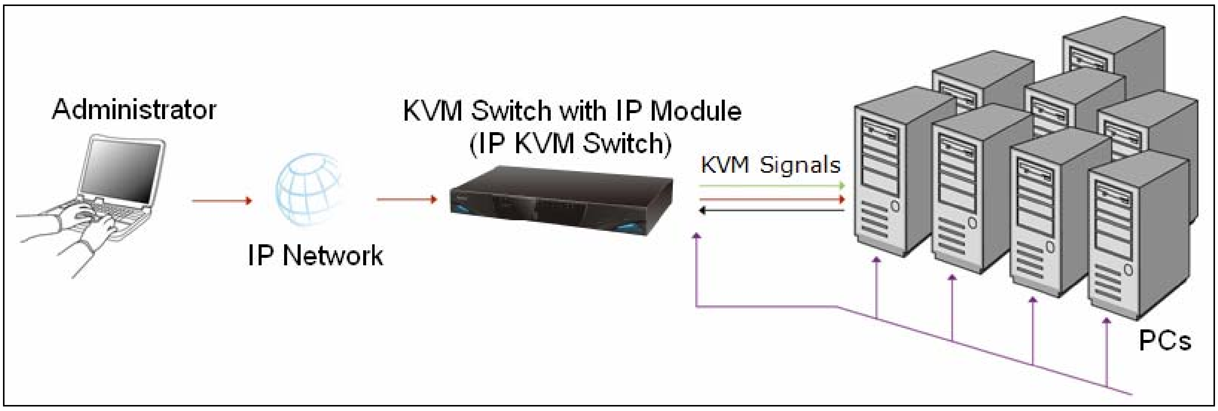
2 Hardware Installation



Follow the steps below to install the module in your KVM Switch:

1. Power off your KVM switch.
2. Remove the screw to open the back cover of module slot.
3. Slide the module card into the slot and secure it to KVM switch.
4. (Optional) Connect the type A connector of USB A-mini B cable to the host computer, while using remote mass storage control.
5. Connect the Ethernet cable to LAN port or the modem to serial port, depending on how you want to access IP KVM switch.
6. Power on your KVM switch.

Congratulations! You have transformed your KVM switch into an IP KVM switch. The figure below shows the connections of IP KVM switch application.



3 Getting Started

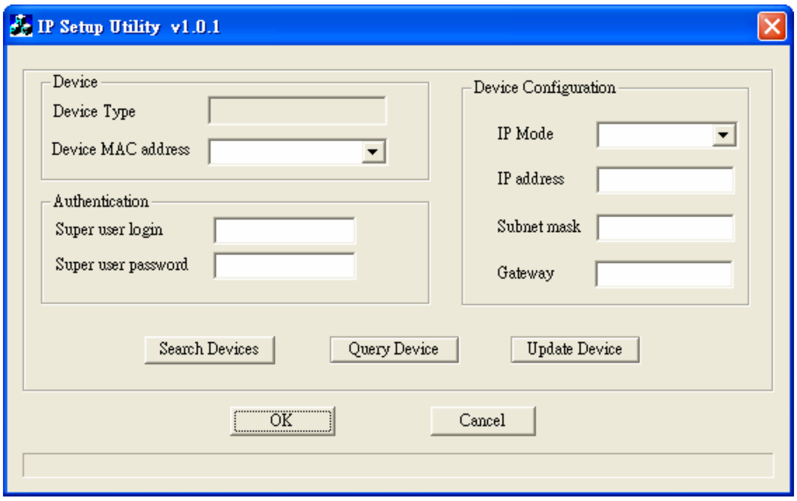
3.1 Initial Configuration

In addition to VT100 interface, we also provide a Network Setup Software tool (IP Setup Utility) for the network settings to the IP KVM. The factory default settings are:

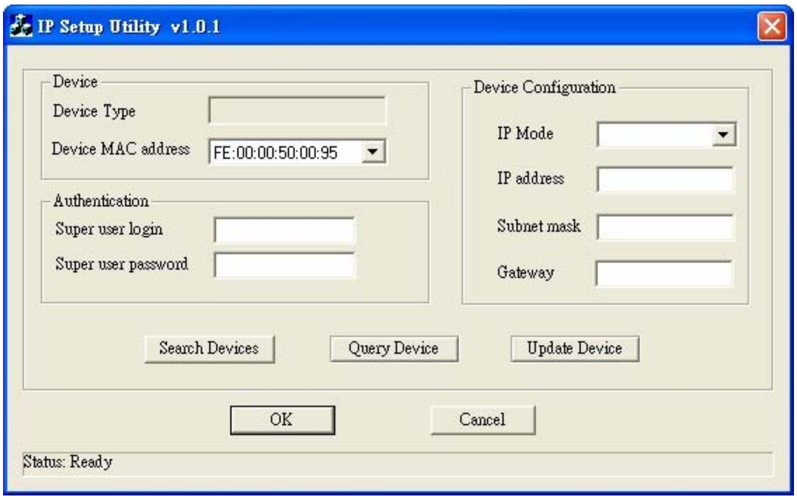
Parameter	Value
DHCP	Disable
IP Address	192.168.0.1
Subnet Mask	255.255.255.0

The IP Setup Utility is useful when setting up the network configuration (IP address, Subnet mask, DHCP, etc). **IpSetup** tool can be found in the CD-ROM shipped with package. You can view or change the network settings via this utility.
Follow the description below to setup your IP KVM switch.

1. Connect the IP KVM switch to your computer via local network (Ethernet cable).
2. Run the setup tool **IpSetup.exe** from CD-ROM. A window will display as below.



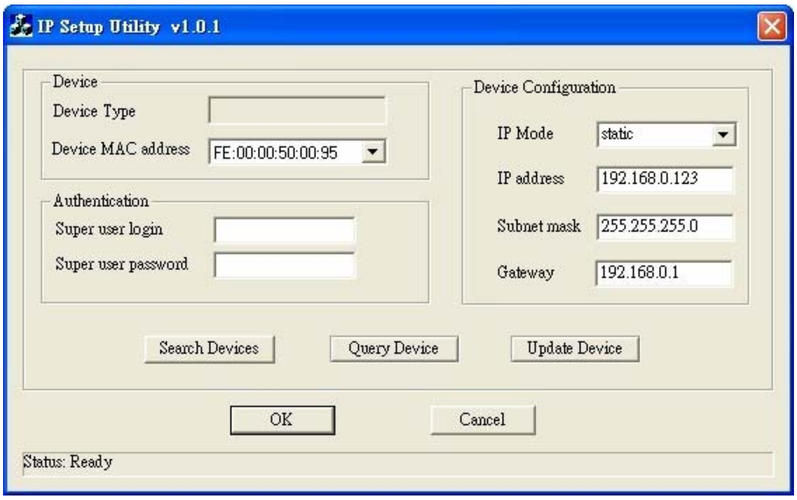
3. The MAC address of IP KVM switch is displayed on Device MAC address field.



Device MAC address FE:00:00:50:00:95

Status: Ready

4. Select the MAC address from Device MAC address and then click **Query Device** to get the device configuration on the right pane.



Device Type:
Device MAC address: FE:00:00:50:00:95
Super user login:
Super user password:
IP Mode: static
IP address: 192.168.0.123
Subnet mask: 255.255.255.0
Gateway: 192.168.0.1
Status: Ready

5. You can then configure the network configuration as DHCP or fixed IP (static). If you want to change the settings.

- **Configuring DHCP**
  Before connecting the IP KVM switch to your local network, be sure to complete the corresponding configuration of the DHCP server.
  Select the “IP Mode” as “DHCP” and obtain the IP address, Subnet mask and gateway from DHCP server automatically.
- **Configuring Fixed IP**
  Select “IP Mode” as “Static” and then configure the IP address, Subnet mask and Gateway.

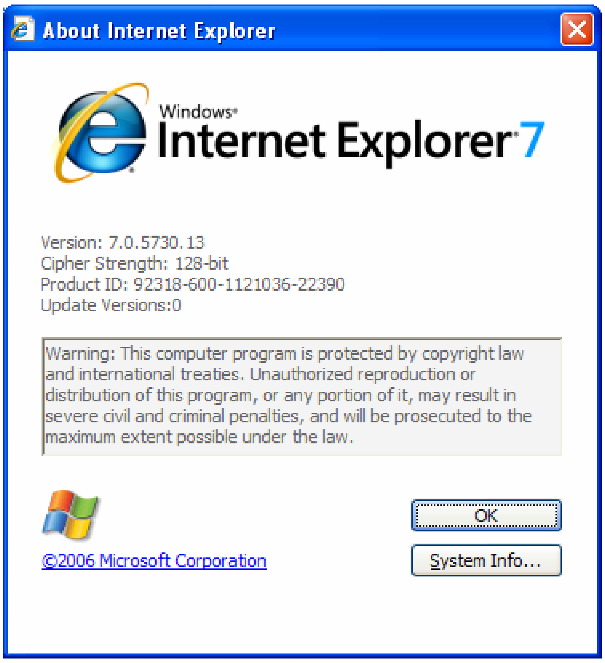
6. Enter the Super user name & password on the left pane. Then click **Update Device**. The new settings will be saved to the IP KVM and the IP KVM will reboot automatically.

Device	
Device Type	The device type of the module card.
Device MAC Address	The MAC address of the IP Module card.
Authentication	
Super User Login	Enter the login name of the super user. The default value is “root” (in lower case).
Super User Password	Enter the login password for the super user. The default value is “superuser” (in lower case).
Device Configuration	
IP Mode	Select the IP configuration mode as static (fixed IP address), dhcp
IP Address	Configure the IP address manually for a fixed IP or obtain a dynamic one from the DHCP server.
Subnet Mask	Configure the subnet mask manually for a fixed IP or obtain it from the DHCP server.
Gateway	Configure the default router manually for a fixed IP or obtain it from the DHCP server.
Search Device	Search for the MAC address of connecting IP Module.
Query Device	Display the current configuration (some firmware versions may require authentication for this action).
Setup Device	To apply the new settings, enter the super user name and its password for “Super user login” and the “Super user password” fields.

3.2 Prerequisites

In order to access the remote host system using a securely encrypted connection, you need a browser that supports the HTTPS protocol. Strong security is only assured by using a key length of 128-Bit. Some of the old browsers do not have a strong 128-bit encryption algorithm. You can access the IP KVM switch using the insecure HTTP protocol, or using the encrypted HTTPS protocol. Whenever possible, use HTTPS.

For Windows Internet explorer users, to check to encryption algorithm, open the “About” option from “Help” menu to read the key length that is currently activated. Newer web browsers generally support strong encryption on default.



Version: 7.0.5730.13
Cipher Strength: 128-bit
Product ID: 92318-600-1121036-22390
Update Versions:0

Warning: This computer program is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under the law.

3.3 Installing JVM on Client System

IP KVM switch was accessed using a standard JAVA enabled web browser. You must install Sun JVM 1.6 or above in your client system.

Note: At a minimum you must have Internet Explorer 6.0 (or above) or Firefox 1.0 (or above) installed on your client computer.

4 Login to the IP KVM Switch

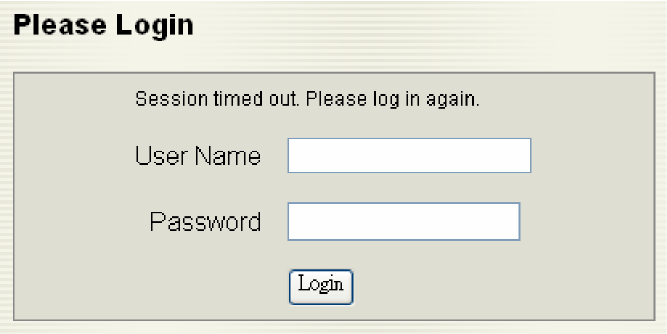
Launch your web browser. The address used might be an IP address or a domain name if you have given your IP KVM a symbolic name in the DNS.
Enter the following address in the URL field of your browser when establishing an unsecured connection:

http://<IP address of IP KVM switch>

Enter the following address in the URL field of your browser when using a secure connection:

http**s**://<IP address of IP KVM switch>

This will lead you to the IP KVM login page as shown below. When connecting to the IP KVM, the IP KVM system (web server) will prompt you to enter the user name and password in order to access to the system.



Please Login

Session timed out. Please log in again.

The IP KVM switch is built-in with a super user that has all permissions to administrate your IP KVM switch. The account (username and password) for super user are:

Username	root (factory default)
Password	superuser (default)

There are two levels of access privileges:

User Name	**Default Password**	**Access Privileges**
root	superuser	full access
(user define)	(user define)	limited access

Warning!!! It is recommended that changing the superuser's password immediately after you login to the IP KVM for the first time. Otherwise, the system may face security risks and unauthorized access to the IP KVM and the host system.

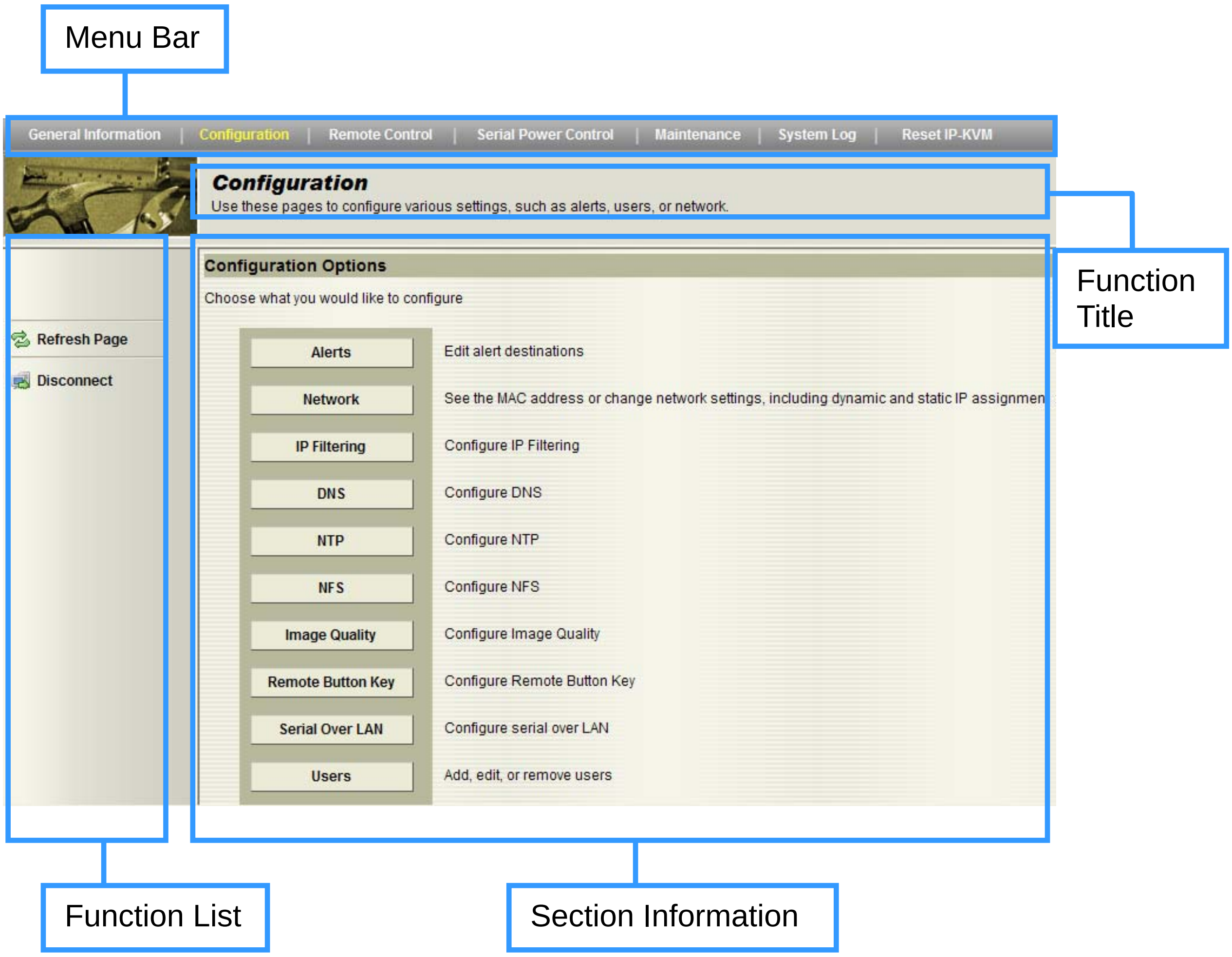
The administrator can add or remove a user easily via the web pages of System administration.
In order to protect IP KVM from unauthorized user access, a session access timeout of 300 seconds is fired or restarted each time the web page configuration is initiated. You will be redirected to login webpage and asked to do account authentication again. The session timeout helps you to prevent from those who do not have access privilege to modify system configuration. In other words, if you leave the web browser idle for more than 300 seconds the login session will time out and thus terminate the session to prevent others from accessing to the IP KVM.

5 Web Browser Management Interface

The IP KVM supports both HTTP and HTTPS (HTTP over SSL) protocols. The users must be authenticated by the system by using the correct user name and password to log into the system.

To access the IP KVM Web management pages, enter the IP KVM's IP address or resolvable hostname into the web browser's URL/Location field. This will direct the user to the IP KVM login screen.

The figure below shows the homepage of the IP KVM Web management interface.



Configuration

Use these pages to configure various settings, such as alerts, users, or network.

Configuration Options

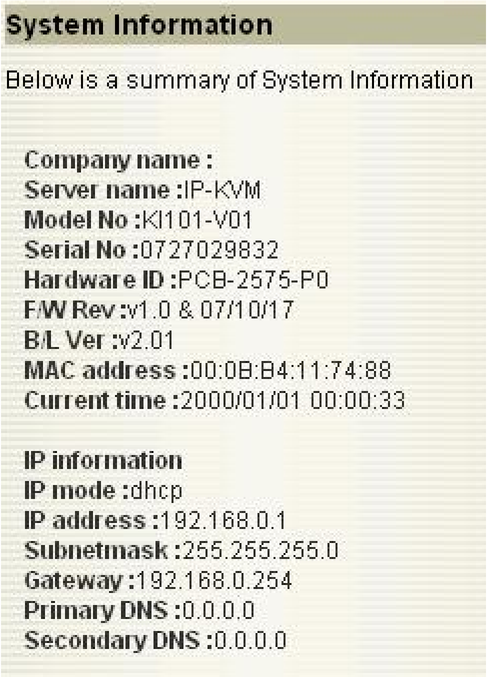
Choose what you would like to configure

Alerts	Edit alert destinations
Network	See the MAC address or change network settings, including dynamic and static IP assignmen
IP Filtering	Configure IP Filtering
DNS	Configure DNS
NTP	Configure NTP
NFS	Configure NFS
Image Quality	Configure Image Quality
Remote Button Key	Configure Remote Button Key
Serial Over LAN	Configure serial over LAN
Users	Add, edit, or remove users

A menu bar displays on the top of the screen. Selecting an item on the menu bar opens a tree view of all the functions available under each grouping. Selecting a function item will allow you to modify its settings.

5.1 General Information

This page lists the system information of the IP KVM. It is the homepage after logging to the unit.



System Information

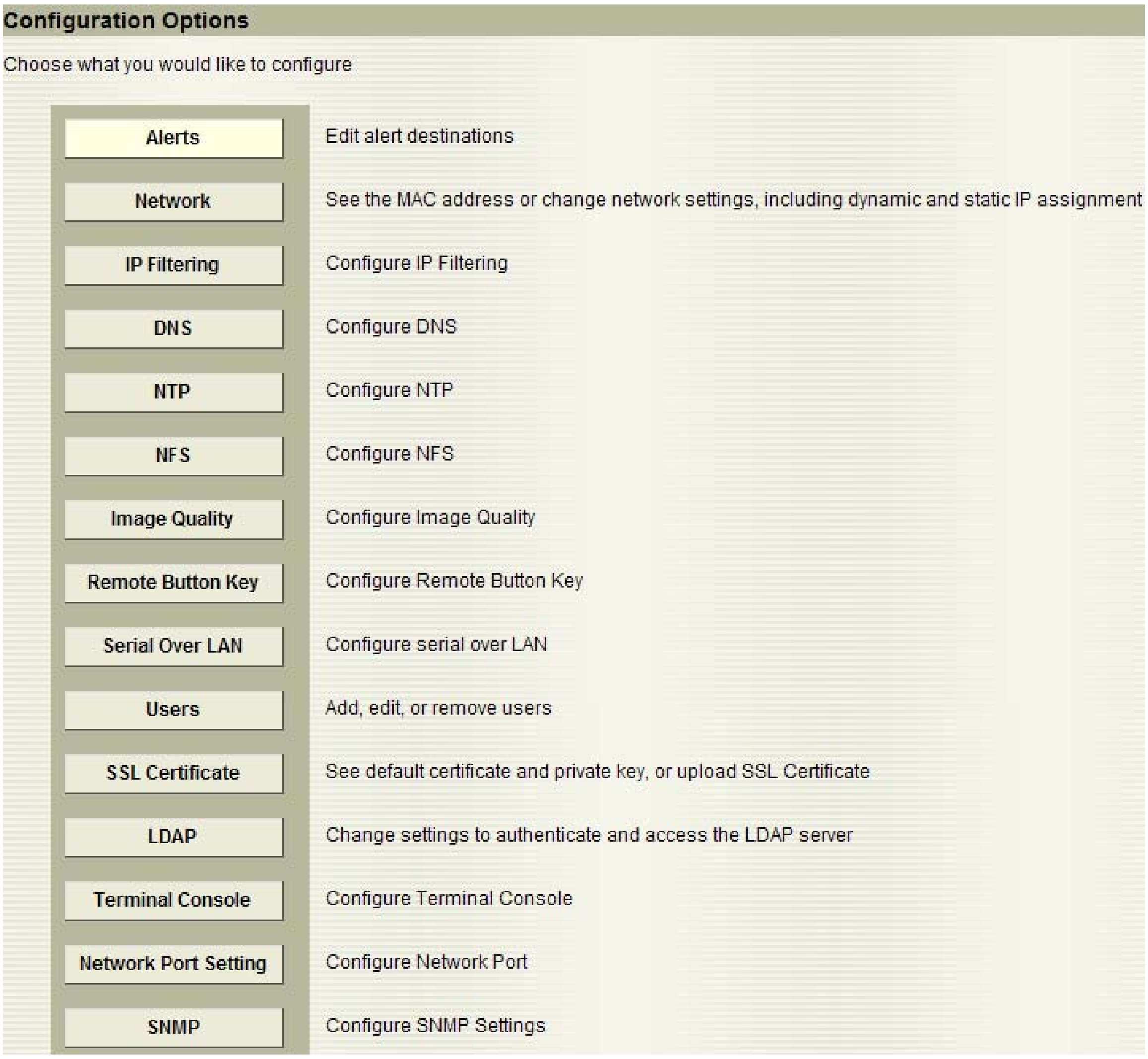
Below is a summary of System Information

Company name :
Server name :IP-KVM
Model No :KI101-V01
Serial No :0727029832
Hardware ID :PCB-2575-P0
F/W Rev :v1.0 & 07/10/17
B/L Ver :v2.01
MAC address :00:0B:B4:11:74:88
Current time :2000/01/01 00:00:33

IP information
IP mode :dhcp
IP address :192.168.0.1
Subnetmask :255.255.255.0
Gateway :192.168.0.254
Primary DNS :0.0.0.0
Secondary DNS :0.0.0.0

5.2 Configuration

This page lists the options of configuration. Choose the item you would like to configure.



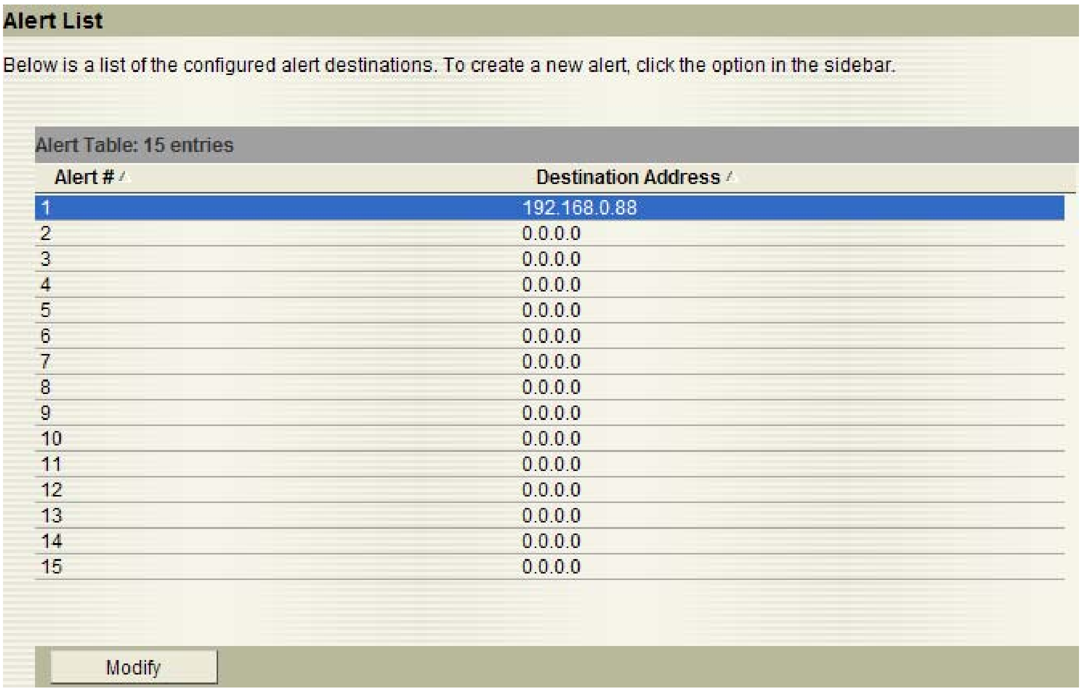
Configuration Options

Choose what you would like to configure

Alerts	Edit alert destinations
Network	See the MAC address or change network settings, including dynamic and static IP assignment
IP Filtering	Configure IP Filtering
DNS	Configure DNS
NTP	Configure NTP
NFS	Configure NFS
Image Quality	Configure Image Quality
Remote Button Key	Configure Remote Button Key
Serial Over LAN	Configure serial over LAN
Users	Add, edit, or remove users
SSL Certificate	See default certificate and private key, or upload SSL Certificate
LDAP	Change settings to authenticate and access the LDAP server
Terminal Console	Configure Terminal Console
Network Port Setting	Configure Network Port
SNMP	Configure SNMP Settings

5.2.1 Alerts

This page allows you to configure the system alert destinations.



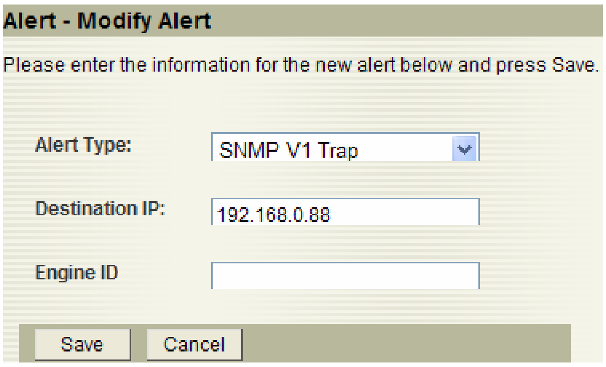
Alert List

Below is a list of the configured alert destinations. To create a new alert, click the option in the sidebar.

Alert Table: 15 entries

Alert #	Destination Address
1	192.168.0.88
2	0.0.0.0
3	0.0.0.0
4	0.0.0.0
5	0.0.0.0
6	0.0.0.0
7	0.0.0.0
8	0.0.0.0
9	0.0.0.0
10	0.0.0.0
11	0.0.0.0
12	0.0.0.0
13	0.0.0.0
14	0.0.0.0
15	0.0.0.0

To configure a new alert, select the entry and click Modify button. The configuration page will display as below.



Alert - Modify Alert

Please enter the information for the new alert below and press Save.

Alert Type: SNMP V1 Trap

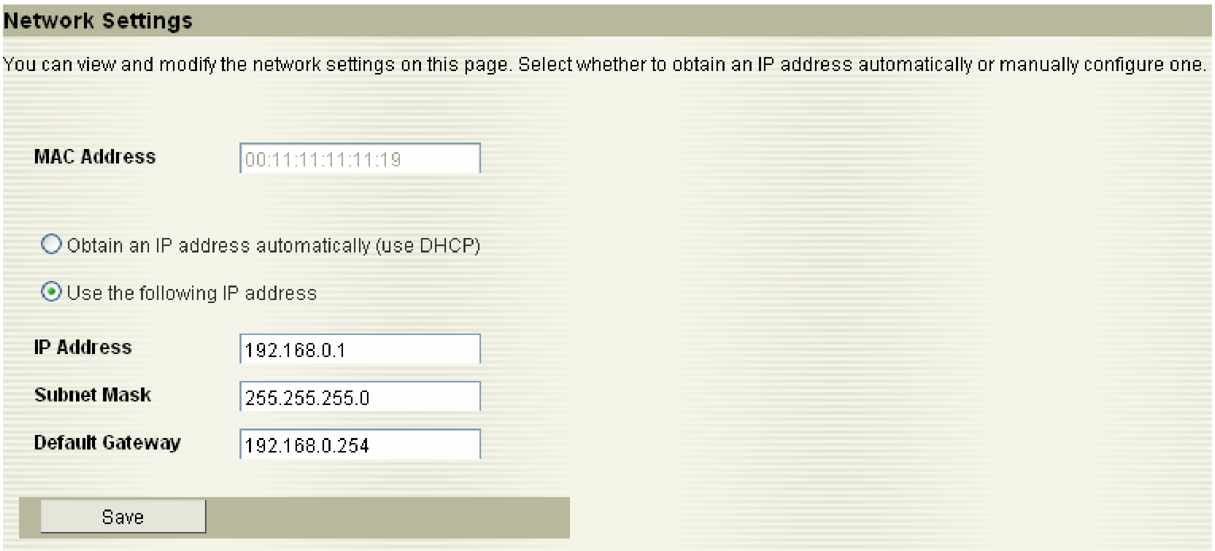
Destination IP: 192.168.0.88

Engine ID

Item	Description
Alert Type	Select the type of the alert.
Destination IP	Enter the IP address of the system that alerts will be sent.
Engine ID	Enter the unique identifier of a SNMP engine.

5.2.2 Network

This page allows you to configure the network settings. The IP KVM requires a valid IP address to operate within the user's network. If the IP address is not readily available, contact the system administrator to obtain a valid IP address for the IP KVM. Please note that the IP KVM requires a unique IP address to connect to the user's network.



Network Settings

You can view and modify the network settings on this page. Select whether to obtain an IP address automatically or manually configure one.

MAC Address: 00:11:11:11:11:19

○ Obtain an IP address automatically (use DHCP)

● Use the following IP address

IP Address: 192.168.0.1

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.0.254

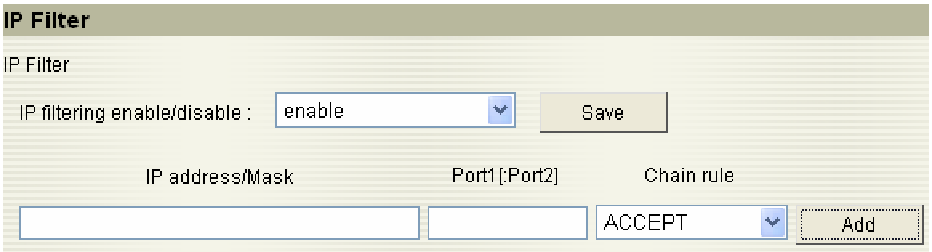
There are two types of IP assignments user can choose from:

- Static IP
- DHCP (Dynamic Host Configuration Protocol)

The IP KVM is initially defaulted to Static IP mode, with a static IP address of 192.168.0.1. The IP configuration setting will not take effect until clicking the **Save** button.

5.2.3 IP Filter

This page allows you to configure IP filter settings. The IP filter keeps unauthorized hosts from accessing to the IP KVM by specifying IP filter rules. It is important to correctly understand what an IP filter is. Otherwise, you might get unexpected results against your original plan.

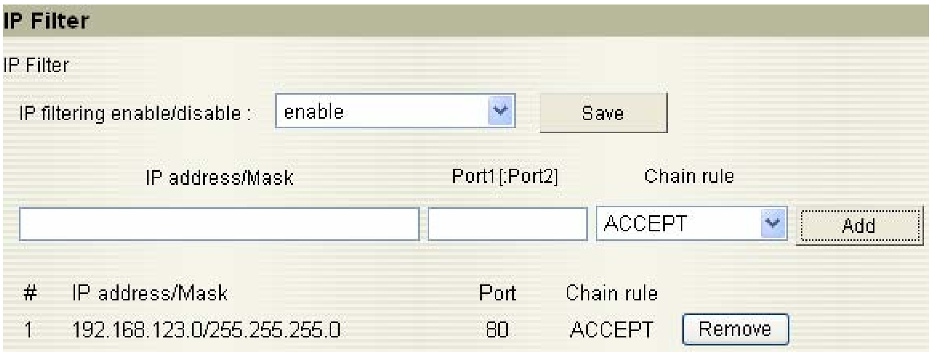


IP Filter

IP Filter

IP filtering enable/disable : enable

IP address/Mask	Port1 [:Port2]	Chain rule
		ACCEPT



IP Filter

IP Filter

IP filtering enable/disable : enable

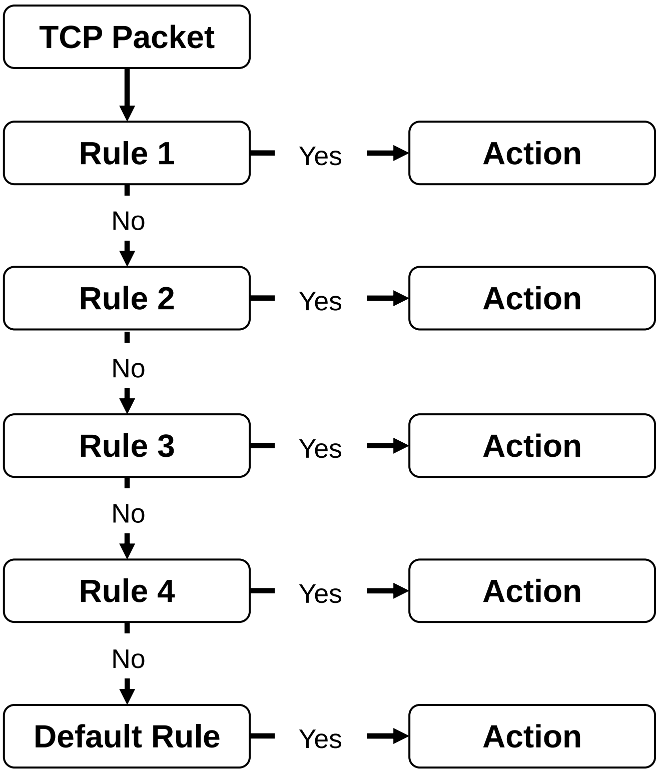
#	IP address/Mask	Port	Chain rule
1	192.168.123.0/255.255.255.0	80	ACCEPT

The **IP address/Mask** specifies the host range by entering host IP address followed by **/** and subnet mask. The host IP addresses will be filtered are based on the rules defined. The table below gives examples of IP address/Mask settings.

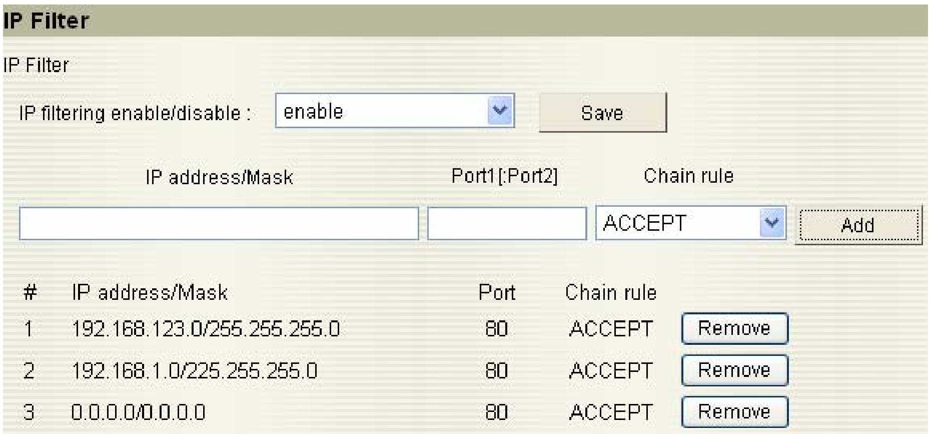
Specified Host Range	Host IP Address	Subnet Mask
Any host	0.0.0.0	0.0.0.0
192.168.1.120	192.168.1.120	255.255.255.255
192.168.1.1 ~ 192.168.1.254	192.168.1.0	255.255.255.0
192.168.0.1 ~ 192.168.255.254	192.168.0.0	255.255.0.0
192.168.1.1 ~ 192.168.1.126	192.168.1.0	255.255.255.128
192.168.1.129 ~ 192.168.1.254	192.168.1.128	255.255.255.128

Item	Description
IP filtering enable/disable	Select to enable or disable IP filtering.
IP address/Mask	Enter the IP address and subnet mask for the rule.
Port1[:Port2]	Enter the port number or port range of the IP KVM which hosts try to access to.
Chain Rule	Select if the access from the hosts will be allowed (ACCEPT) or denied (DROP).

When the IP KVM receives a TCP packet, it will process the packet with the chain rule depicted below. The packet will be matched with the chain rule 1 first. The system will take action directly if the packet meets the chain rule 1, otherwise, go to chain rule 2.



You can add a new IP filtering rule by setting the properties and then click the **Add** button. To delete an existing rule, just click the **Remove** button next the rule.



IP Filter

IP Filter

IP filtering enable/disable : enable

IP address/Mask	Port1[:Port2]	Chain rule
		ACCEPT

#	IP address/Mask	Port	Chain rule	
1	192.168.123.0/255.255.255.0	80	ACCEPT	Remove
2	192.168.1.0/225.255.255.0	80	ACCEPT	Remove
3	0.0.0.0/0.0.0.0	80	ACCEPT	Remove

In the example above, the rules applied in the following order:

#1. Those hosts belonging to subnet 192.168.123.x are allowed to access to the IP KVM (through http port 80).
#2. Those hosts belonging to subnet 192.168.1.x are allowed to access to the IP KVM (through http port 80).
#3. All hosts are allowed to access to the IP KVM (through http port 80).

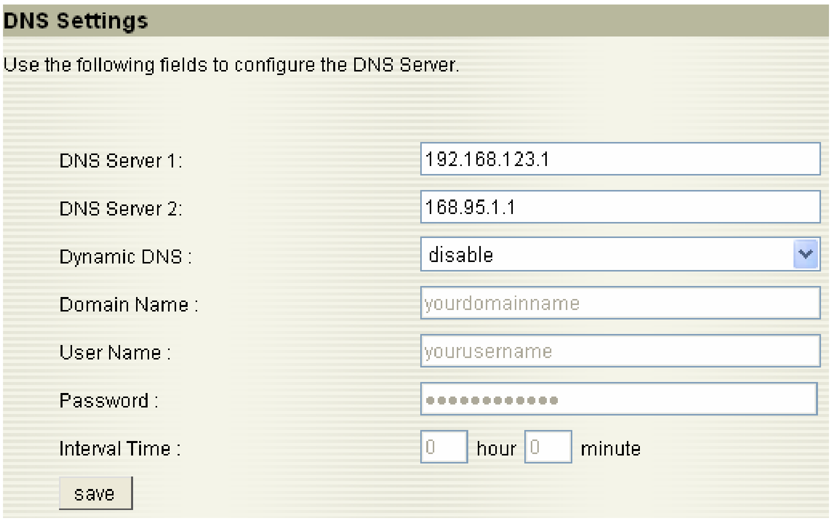
After these three rules applied, only the hosts which belong to the subnet 192.168.1.x or 192.168.123.x can access to the IP KVM (through http port 80).

5.2.4 DNS

This page allows you to configure DNS (Domain Name System) and DDNS (Dynamic DNS) settings. The DNS is the Internet service that translates your domain names into IP addresses. When you connect the IP KVM to a DSL line or use a DHCP configuration and get a dynamic IP address from the network, the IP address may not the same as previous connection. Therefore, it is difficult to know if an IP address has changed or what the new IP address is. A Dynamic DNS service is provided by various ISPs or organizations to deal with this situation. By using the Dynamic DNS service, you can access the IP KVM through the hostname registered in the Dynamic DNS Server regardless of any IP address change. The IP KVM only supports Dynamic DNS service offered at Dynamic DNS Network Services (http://www.dyndns.org).

To use the Dynamic DNS service provided by Dynamic DNS Network Services, you must set up an account in their Members' NIC (Network Information Center - http://members.dyndns.org). You may then add a new Dynamic DNS Host link after logging in to their Dynamic DNS Network Services Members NIC.

After enabling the Dynamic DNS service in the Dynamic DNS Configuration menu, you must enter the registered Domain Name, User Name and Password. After applying the configuration change, you can access the IP KVM using only the Domain Name.



DNS Settings

Use the following fields to configure the DNS Server.

DNS Server 1: 192.168.123.1

DNS Server 2: 168.95.1.1

Dynamic DNS : disable

Domain Name : yourdomainname

User Name : yourusername

Password : ●●●●●●●●●●●●

Interval Time : 0 hour 0 minute

Item	Description
DNS Server 1/2	Enter the IP address of DNS server(s).
Dynamic DNS	Select to enable or disable DDNS.
Domain Name	Enter the domain name of your DDNS account.
User Name	Enter the user name of your DDNS account.
Password	Enter the password of your DDNS account.
Interval Time	Enter the time interval after which DDNS server should check and update the IP address of your server if changed.

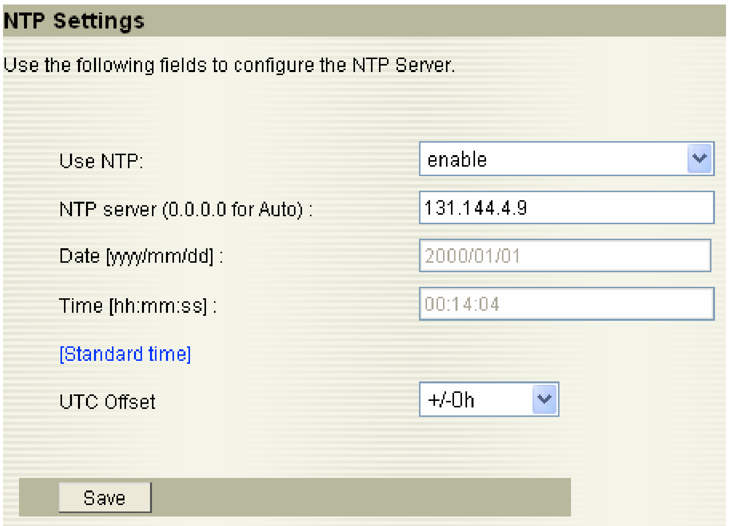
5.2.5 NTP (Date and Time)

This page allows you to manually configure the NTP (Network Time Protocol) server. The IP KVM maintains current date and time information and these are backed up by internal battery power. You can set the time and date either by NTP or specify them manually.

If the NTP feature is enabled, the IP KVM will obtain the date and time information from the NTP server at each reboot, then automatically align with the NTP server time every hour. If the NTP server is set to 0.0.0.0, the IP KVM will automatically use the default NTP servers. In this case, the IP KVM should be connected from the network to the Internet.

The second method is to set date and time manually without using the NTP server. This will allow the date and time information to be kept maintained by the internal battery backup.

You must also specify the time zone, Greenwich Mean Time (GMT), if you use NTP to obtain the time and date. This time is also known as Universal Time (UTC). You also need to set the time offset from UTC depending on your location. You system will then be able to calculate the correct date and time. Please refer to the website http://time_zone.tripod.com for the time offset from UTC.



NTP Settings

Use the following fields to configure the NTP Server.

Use NTP: enable

NTP server (0.0.0.0 for Auto) : 131.144.4.9

Date [yyyy/mm/dd] : 2000/01/01

Time [hh:mm:ss] : 00:14:04

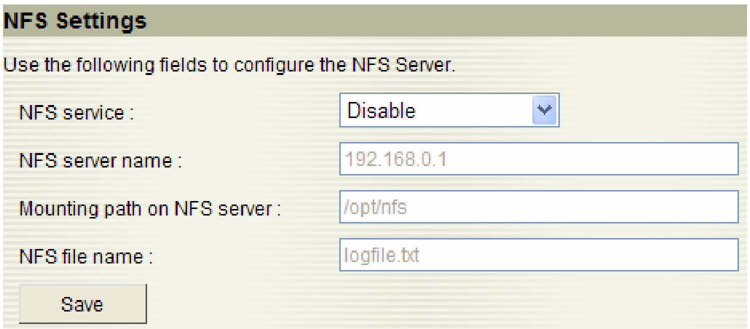
[Standard time]

UTC Offset +/-0h

Item	Description
Use NTP	Select to enable or disable NTP Server.
NTP Server	Enter the IP address of a NTP server or enter 0.0.0.0 for auto detection.
Date	Enter the date manually if the Use NTP function is disabled.
Time	Enter the time manually if the Use NTP function is disabled.
UTC Offset	Select the UTC (Coordinated Universal Time) offset from the drop-down list according to your location.

5.2.6 NFS (Network File System)

This page allows you to configure the NFS function. The IP KVM supports NFS (Network File System) service for system or port data logging.



NFS Settings

Use the following fields to configure the NFS Server.

NFS service : Disable

NFS server name : 192.168.0.1

Mounting path on NFS server : /opt/nfs

NFS file name : logfile.txt

Item	Description
NFS Service	Select to enable or disable NFS Service.
NFS Server Name	Enter the IP address of NFS server.
Mounting Path on NFS Server	Enter the mounting path of NFS server.
NFS File Name	Enter the file name and extension name of NFS file.

5.2.7 Image Quality

This page shows the video image quality level.

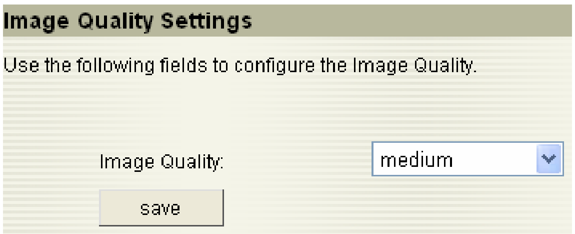


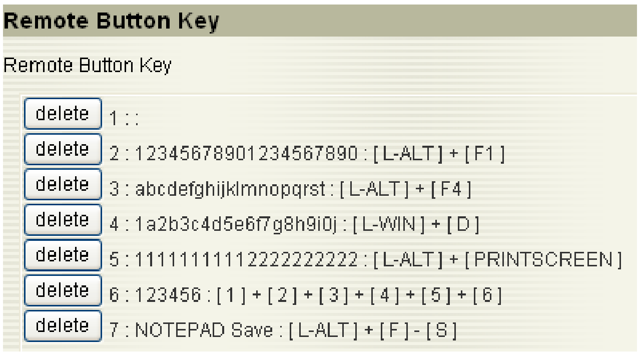
Image Quality Settings

Use the following fields to configure the Image Quality.

Image Quality: medium

5.2.8 Remote Button Key

This page allows you to configure the remote button keys. Remote button keys are used to simulate keystrokes on the remote console and send the concatenated key codes to the remote host computer. This function is to prevent the key code from being captured or blocked by the local operating system or the downstream KVM switch. Typical examples are “Ctrl+Alt+Delete” on Windows and DOS or “Ctrl+Backspace” on Unix or Unix-like OS for terminating the X-Server.



Remote Button Key

Remote Button Key

1 : :

2 : 12345678901234567890 : [L-ALT] + [F1]

3 : abcdefghijklmnopqrst : [L-ALT] + [F4]

4 : 1a2b3c4d5e6f7g8h9i0j : [L-WIN] + [D]

5 : 11111111112222222222 : [L-ALT] + [PRINTSCREEN]

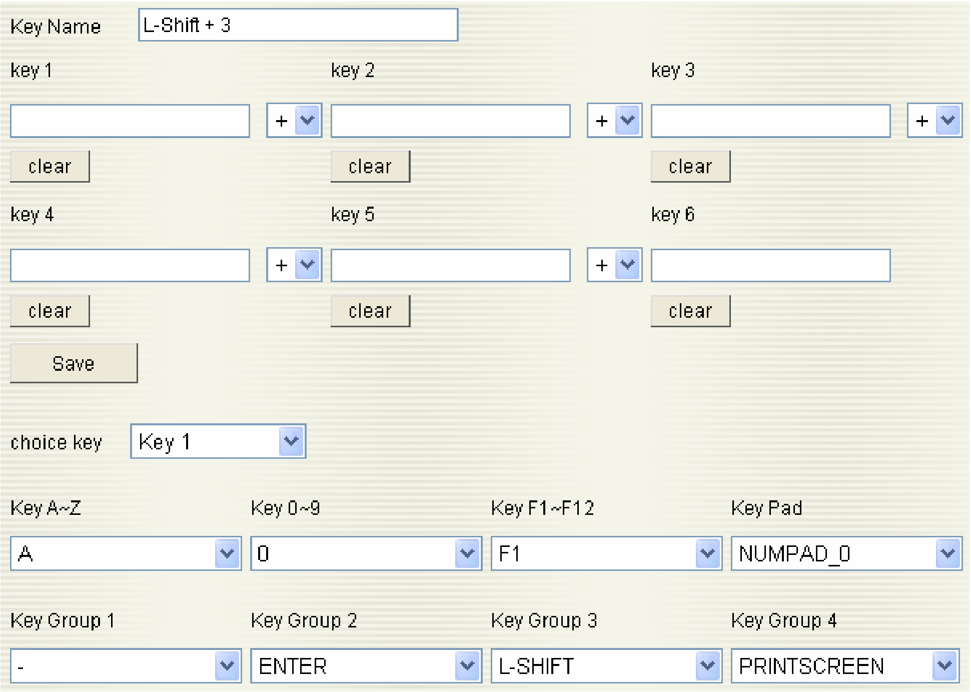
6 : 123456 : [1] + [2] + [3] + [4] + [5] + [6]

7 : NOTEPAD Save : [L-ALT] + [F] - [S]

Multiple key codes can be concatenated.
Here are examples for configure the remote button key.

Example 1:
When you want to define a keystroke of **L-Shift + F3**:

1. Enter the **Key Name** that stands for the key strokes combination.



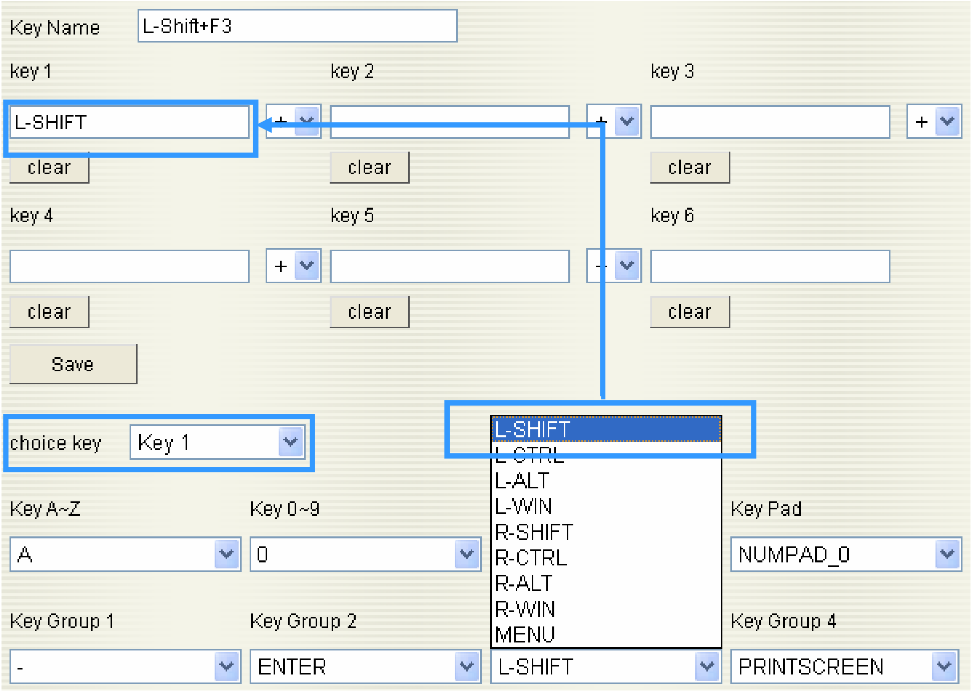
Key Name: L-Shift + 3

choice key: Key 1

Key A~Z	Key 0~9	Key F1~F12	Key Pad
A	0	F1	NUMPAD_0

Key Group 1	Key Group 2	Key Group 3	Key Group 4
-	ENTER	L-SHIFT	PRINTSCREEN

2. Select **choice key 1**: Select **L-SHIFT** from the **Key 1** drop-down list.



Key Name: L-Shift+F3

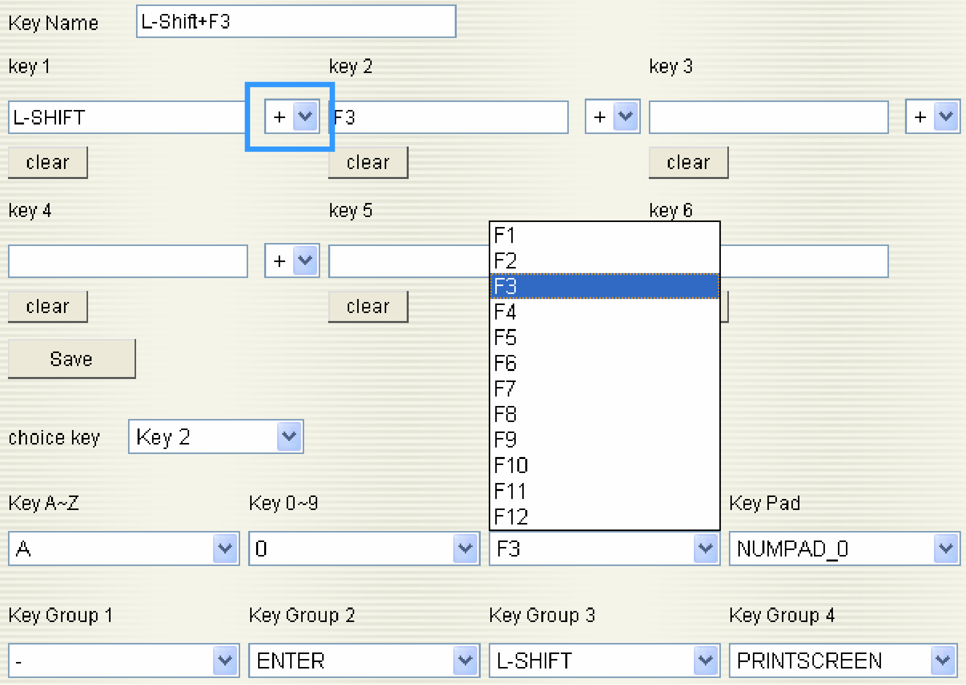
key 1: L-SHIFT

choice key: Key 1

Key A~Z	Key 0~9	Key Pad
A	0	NUMPAD_0

Key Group 1	Key Group 2	Key Group 3	Key Group 4
-	ENTER	L-SHIFT	PRINTSCREEN

3. Select **conjunction key**: Select “**+**” to be the conjunction key from the drop-down list.



Key Name: L-Shift+F3

key 1: L-SHIFT + | key 2: F3 + | key 3: +

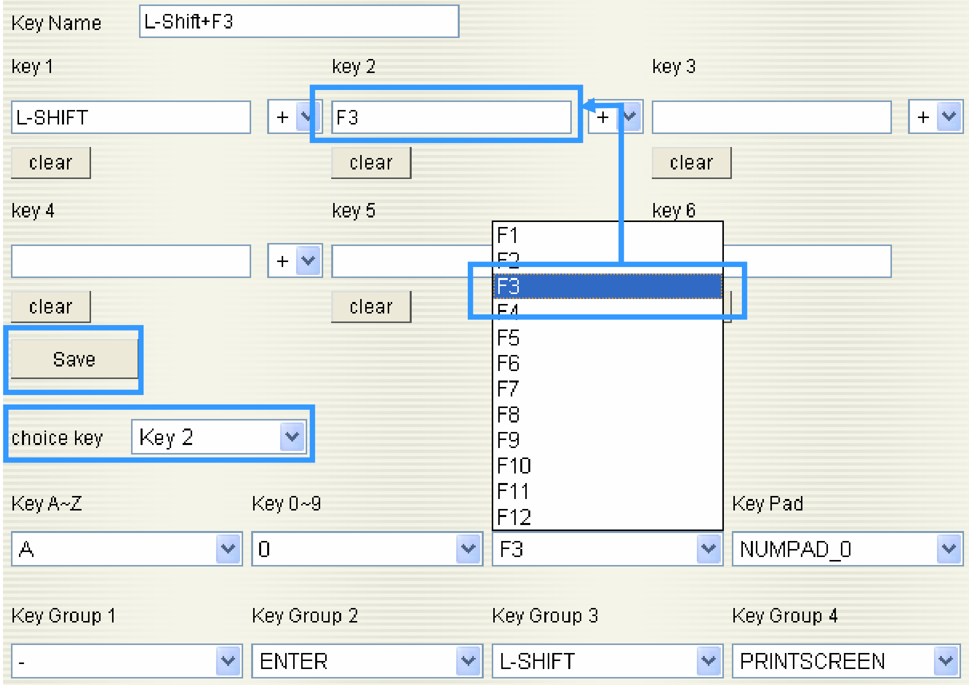
key 4: + | key 5: | key 6:

choice key: Key 2

Key A~Z: A | Key 0~9: 0 | F3 | Key Pad: NUMPAD_0

Key Group 1: - | Key Group 2: ENTER | Key Group 3: L-SHIFT | Key Group 4: PRINTSCREEN

4. Select **choice key 2**: Select **F3** from the **Key 2** drop-down list. Click **Save** to complete the setting.



Key Name: L-Shift+F3

key 1: L-SHIFT + | key 2: F3 + | key 3: +

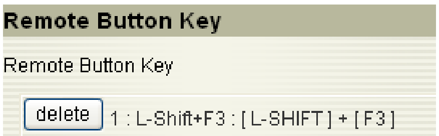
key 4: + | key 5: | key 6:

choice key: Key 2

Key A~Z: A | Key 0~9: 0 | F3 | Key Pad: NUMPAD_0

Key Group 1: - | Key Group 2: ENTER | Key Group 3: L-SHIFT | Key Group 4: PRINTSCREEN

You will see the created button key is showing on top of the page. To trigger this remote button key, you have to press **Light Shift** key and **F3** function key on keyboard simultaneously.



Remote Button Key

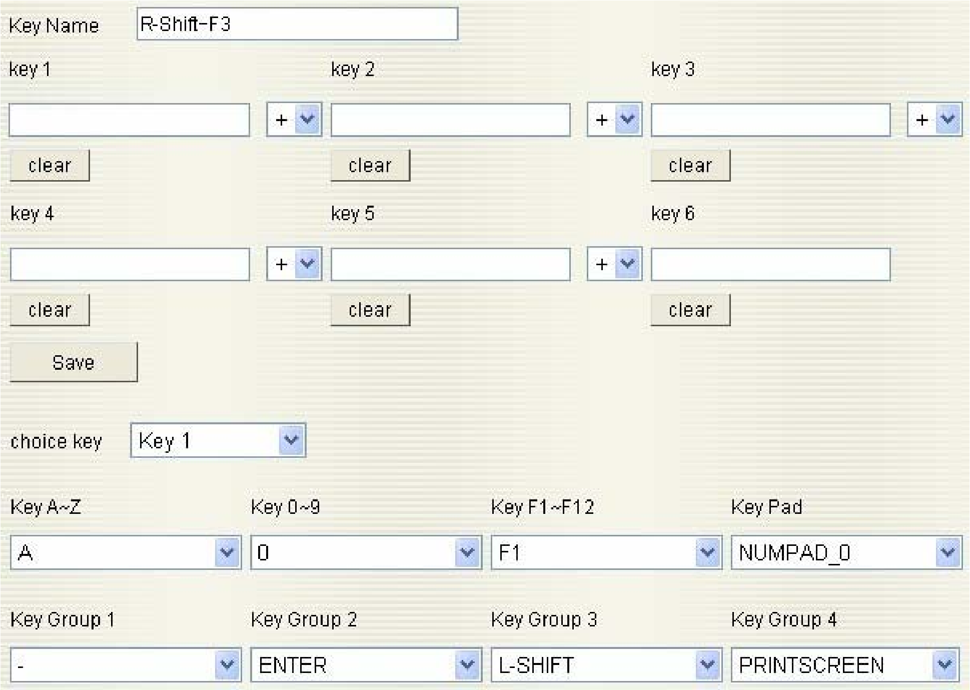
Remote Button Key

delete 1 : L-Shift+F3 : [L-SHIFT] + [F3]

Example 2:

When you want to define a keystroke of **R-Shift - F3**:

1. Enter the **Key Name** that stands for the key strokes combination.



Key Name: R-Shift-F3

key 1: (empty) + | key 2: (empty) + | key 3: (empty) +

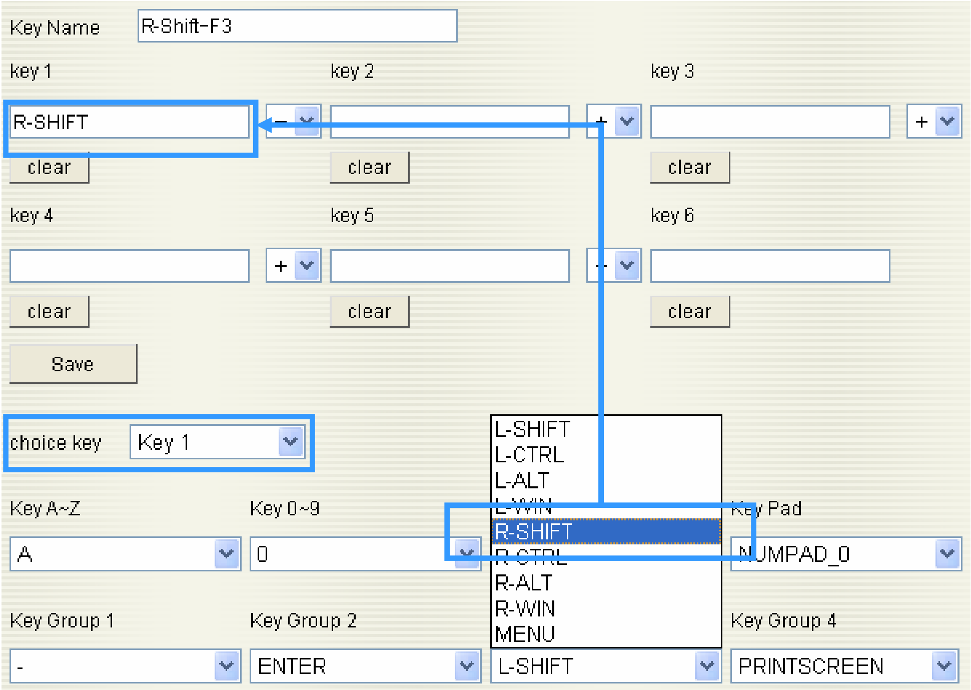
key 4: (empty) + | key 5: (empty) + | key 6: (empty)

choice key: Key 1

Key A~Z	Key 0~9	Key F1~F12	Key Pad
A	0	F1	NUMPAD_0

Key Group 1	Key Group 2	Key Group 3	Key Group 4
-	ENTER	L-SHIFT	PRINTSCREEN

2. Select **choice key 1**: Select **R-SHIFT** from the **Key 1** drop-down list.



Key Name: R-Shift-F3

key 1: R-SHIFT + | key 2: (empty) + | key 3: (empty) +

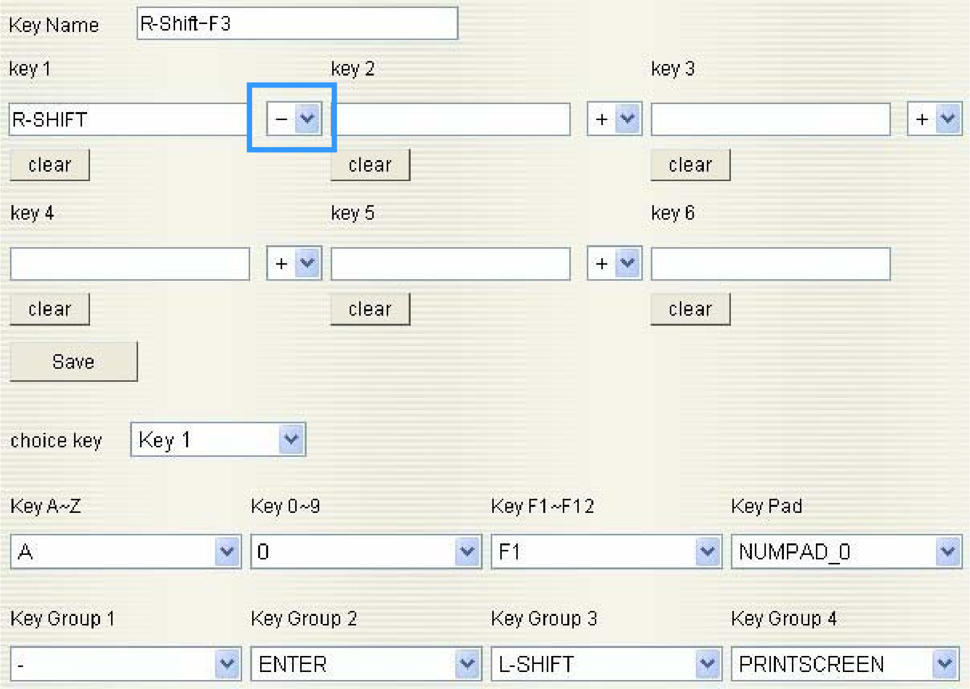
key 4: (empty) + | key 5: (empty) + | key 6: (empty)

choice key: Key 1

Key A~Z	Key 0~9	Key F1~F12	Key Pad
A	0		NUMPAD_0

Key Group 1	Key Group 2	Key Group 3	Key Group 4
-	ENTER	L-SHIFT	PRINTSCREEN

3. Select **conjunction key**: Select "**-**" to be the conjunction key from the drop-down list.



Key Name: R-Shift-F3

key 1: R-SHIFT − key 2: + key 3: +

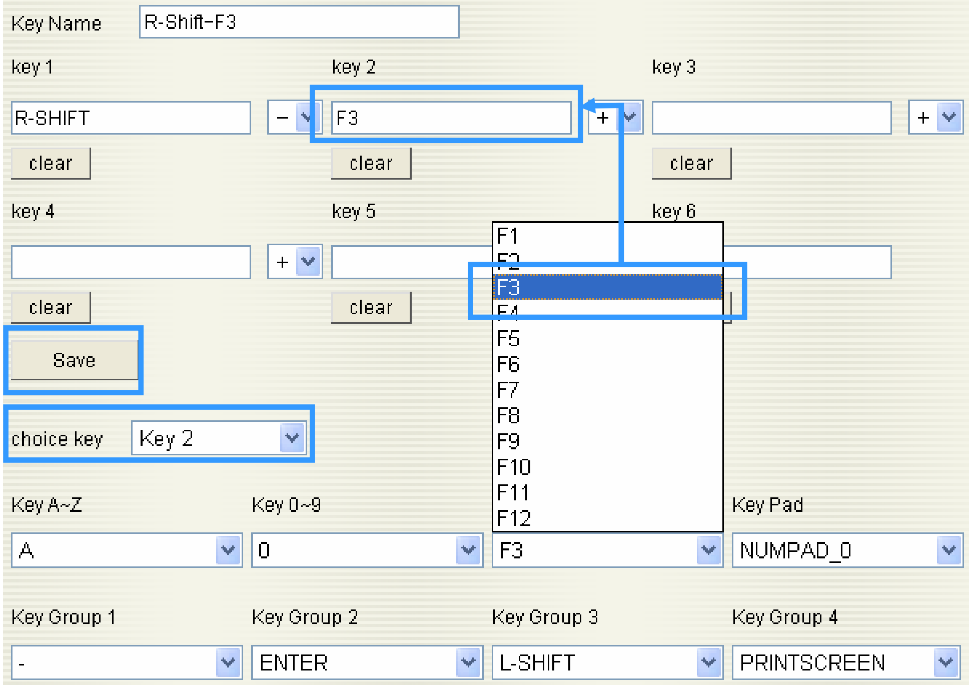
key 4: + key 5: + key 6:

choice key: Key 1

Key A~Z	Key 0~9	Key F1~F12	Key Pad
A	0	F1	NUMPAD_0

Key Group 1	Key Group 2	Key Group 3	Key Group 4
-	ENTER	L-SHIFT	PRINTSCREEN

4. Select **choice key 2**: Select **F3** from the **Key 2** drop-down list. Click **Save** to complete the setting.



Key Name: R-Shift-F3

key 1: R-SHIFT − key 2: F3 + key 3: +

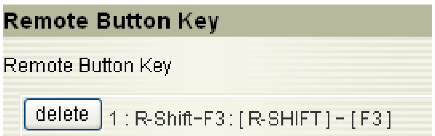
key 4: + key 5: key 6:

choice key: Key 2

Key A~Z	Key 0~9	Key F1~F12	Key Pad
A	0	F3	NUMPAD_0

Key Group 1	Key Group 2	Key Group 3	Key Group 4
-	ENTER	L-SHIFT	PRINTSCREEN

You will see the created button key is showing on top of the page. To trigger this remote button key, you have to press **Right Shift** key and release, then press **F3** function key on keyboard.

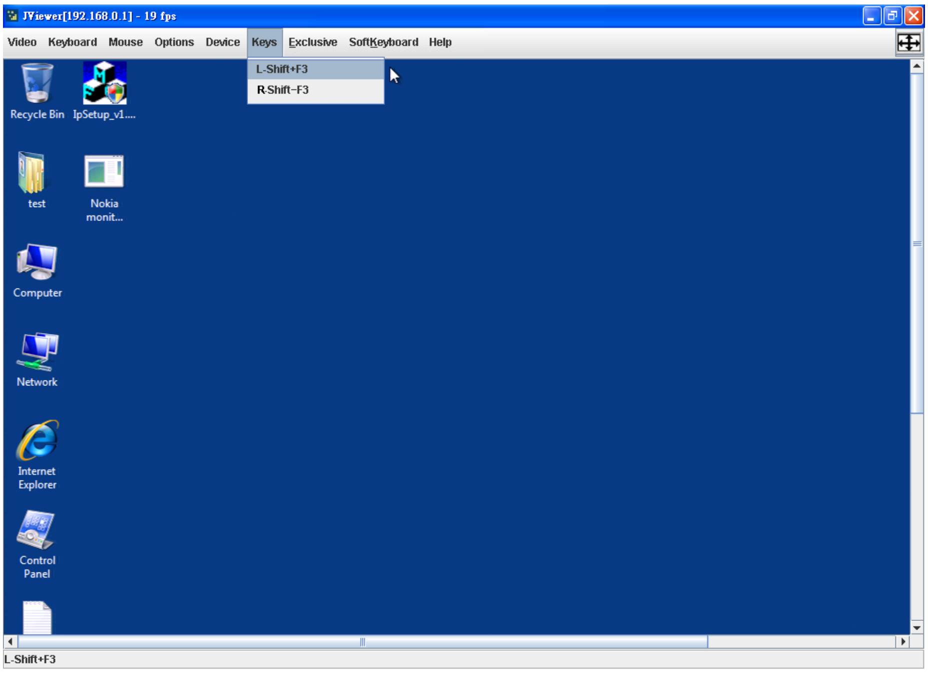


Remote Button Key

Remote Button Key

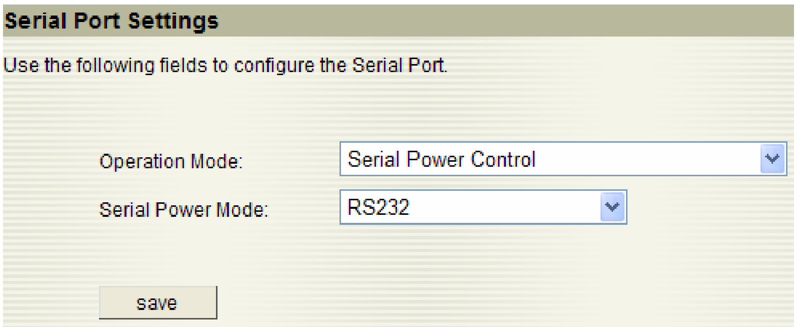
delete 1 : R-Shift-F3 : [R-SHIFT] - [F3]

Open the **Remote KVM Console** (see the section **Remote Control**), you will see the button key **L-Shift + F3** and **R-Shift - F3** are shown on the drop-down menu. Clicking on the button key will send the key codes to the remote host computer.



5.2.9 Serial over LAN

This page allows you to configure the Serial port settings.



Serial Port Settings

Use the following fields to configure the Serial Port.

Operation Mode: Serial Power Control

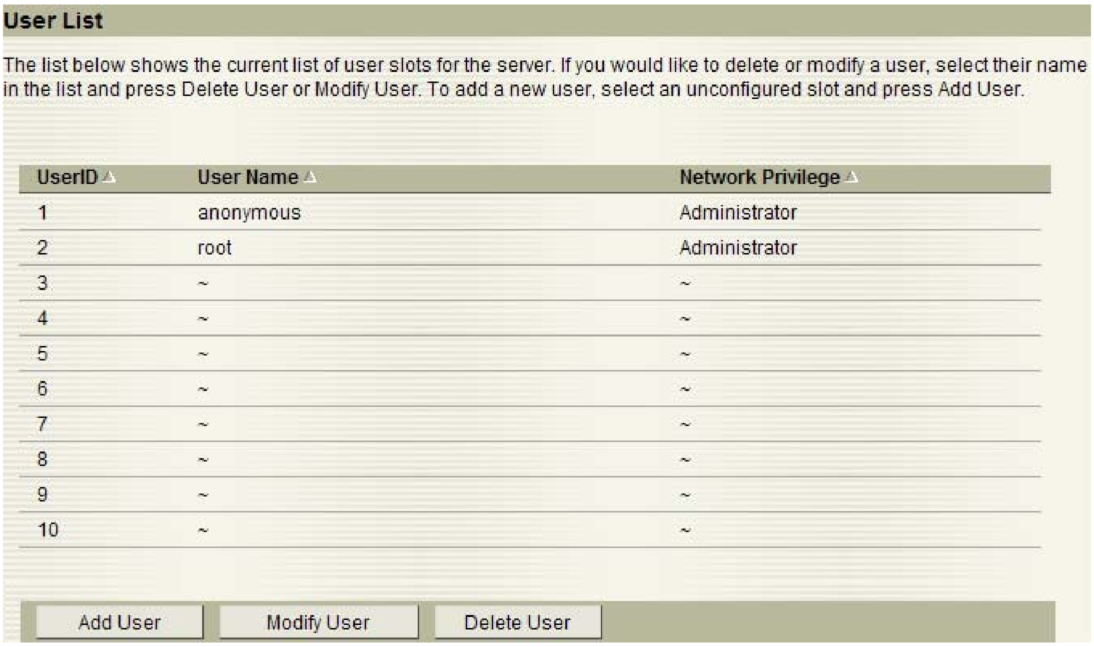
Serial Power Mode: RS232

Item	Description
Operation Mode	Select the operation mode from drop-down list.
Serial Power Mode	Select the serial power mode to be RS232 or RS485.

The Serial Power Controller (SPC) is a family of intelligent power distribution units that enables remote power control of servers and network appliances. When used in conjunction with IP KVM, the SPC provides comprehensive management capabilities and quick problem resolution by integrating console access with power control into a single interface. The SPC supports both RS232 and RS485 interfaces and can be located up to 1.2km away from the controlling master, and has the Daisy chain capability in RS485 mode. Refer to section “Serial Power Control” for more details about Serial Power application.

5.2.10 Users

Administrator can create as many as 10 user accounts for controlling the IP KVM.



User List

The list below shows the current list of user slots for the server. If you would like to delete or modify a user, select their name in the list and press Delete User or Modify User. To add a new user, select an unconfigured slot and press Add User.

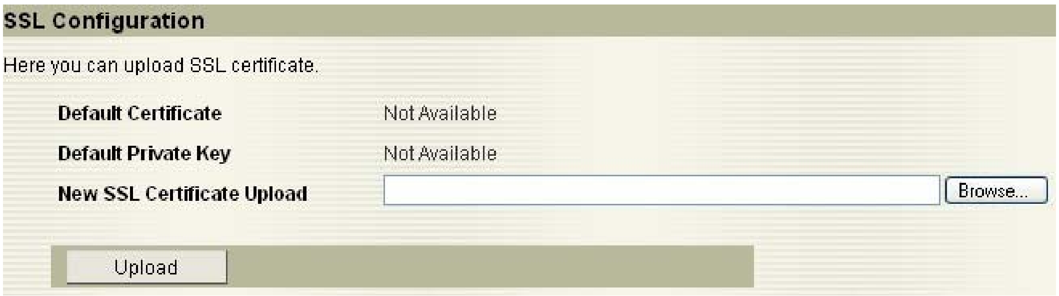
UserID	User Name	Network Privilege
1	anonymous	Administrator
2	root	Administrator
3	~	~
4	~	~
5	~	~
6	~	~
7	~	~
8	~	~
9	~	~
10	~	~

5.2.11 SSL Certificate

This page allows you to configure SSL (Secure Sockets Layer) certificate. A SSL certificate is a digital identification which contains information to attest that certificate belongs to specific person, organization, server or other entity noted in the certificate. IP KVM supports secure HTTP (with the prefix **https://**) to make configuration change via web page. The server side SSL certificate identify IP KVM server itself so that you can rely on the certificate and make the configuration change confidently.

IP KVM is capable of uploading customized certificate files to web server. The certificate file suite includes three files. All three certificate files must be uploaded to complete certificate upgrade. The file upload interface is similar to firmware upgrade. Once all certificate files are uploaded, you have to initiate a reboot command manually to make the new certificate effective.

Browse prepared CA files (follow procedure in Appendix B to prepare CA files with same assigned filenames) and upload those files to IP KVM. Please double check each files before uploading. A false CA file suite may disable secure HTTP function.

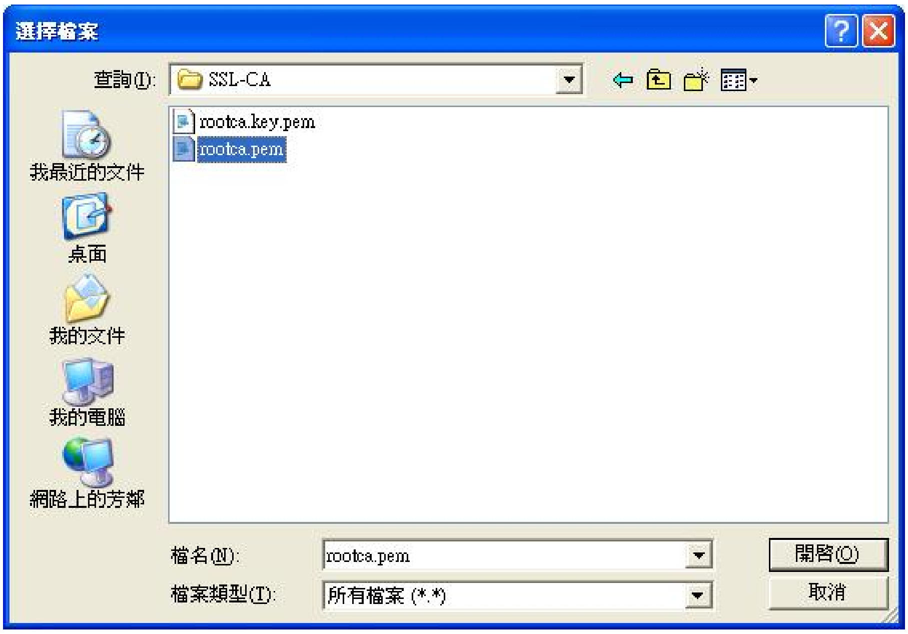


SSL Configuration

Here you can upload SSL certificate.

Default Certificate	Not Available
Default Private Key	Not Available
New SSL Certificate Upload	

1. Click Browse to select the **rootca.pem** as the Default Certificate and click Upload.
2. Click Browse to select the **rootca.key.pem** as the Default Private Key and click Upload.



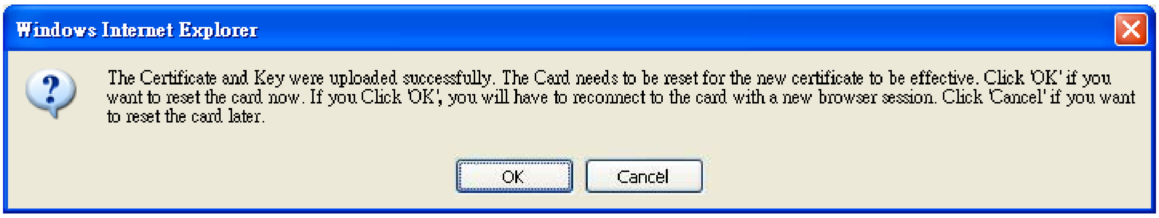
查詢(I): SSL-CA

rootca.key.pem
rootca.pem

檔名(N): rootca.pem

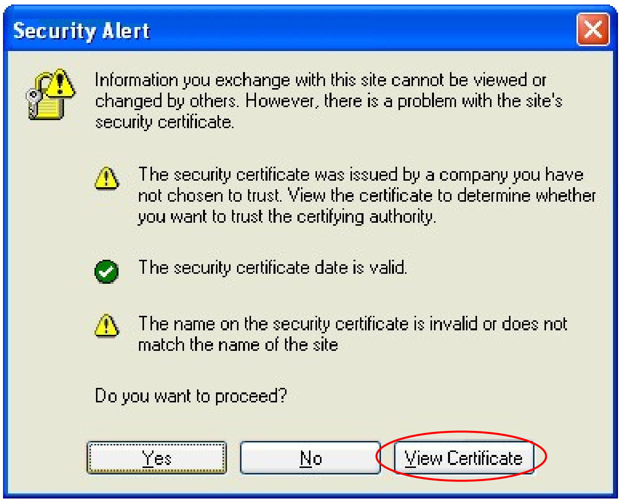
檔案類型(T): 所有檔案 (*.*)

3. Click **OK** to reboot the IP KVM.



The Certificate and Key were uploaded successfully. The Card needs to be reset for the new certificate to be effective. Click 'OK' if you want to reset the card now. If you Click 'OK', you will have to reconnect to the card with a new browser session. Click 'Cancel' if you want to reset the card later.

4. You can then check the Certificates from Windows IE browser **Tools→Internet Options→Contents→Certificates→View**.



Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

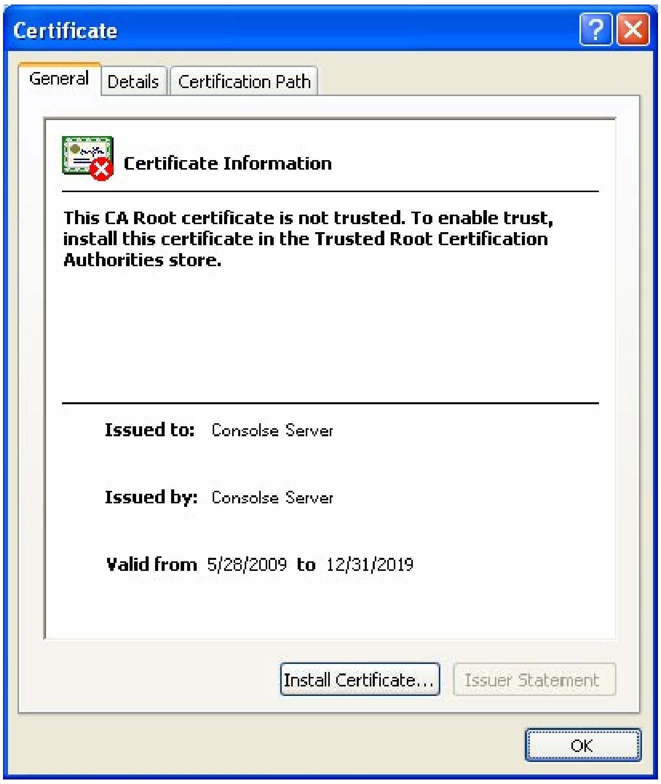
⚠ The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

✓ The security certificate date is valid.

⚠ The name on the security certificate is invalid or does not match the name of the site

Do you want to proceed?

5. Click **Install Certificate** to install the Certificate.



Certificate Information

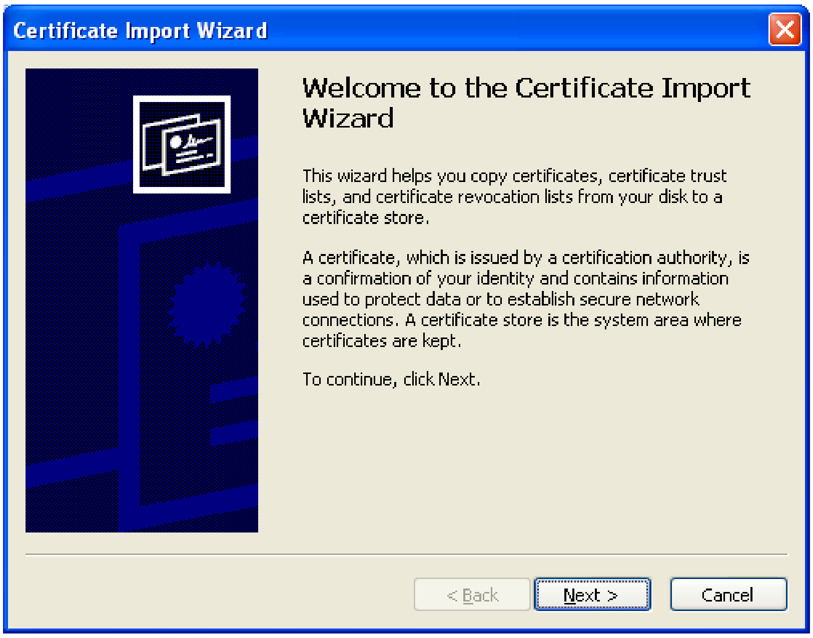
This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: Consolse Server

Issued by: Consolse Server

Valid from 5/28/2009 to 12/31/2019

6. Click **Next** to import the Certificate.



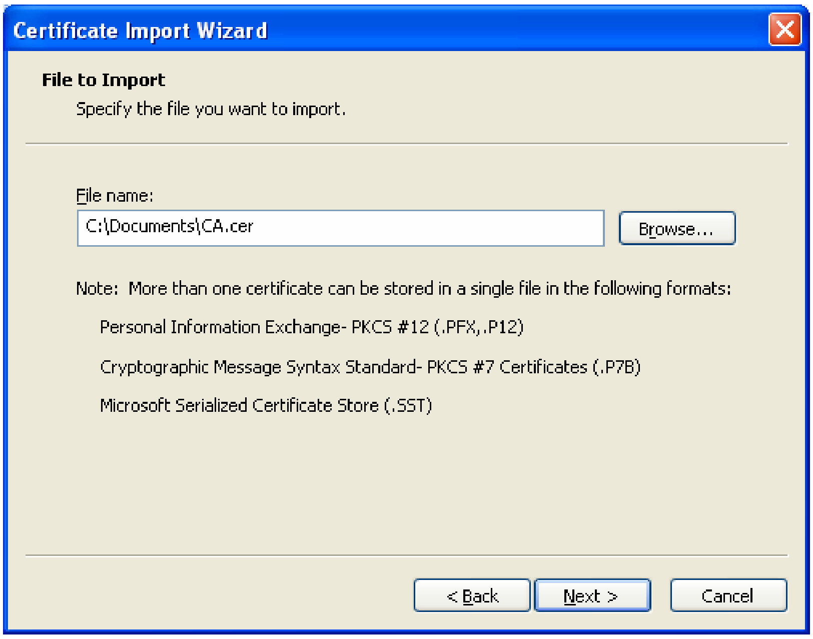
Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

7. Specify t he file you want to import and click **Next** to import the Certificate.



Certificate Import Wizard

File to Import

Specify the file you want to import.

File name:

C:\Documents\CA.cer

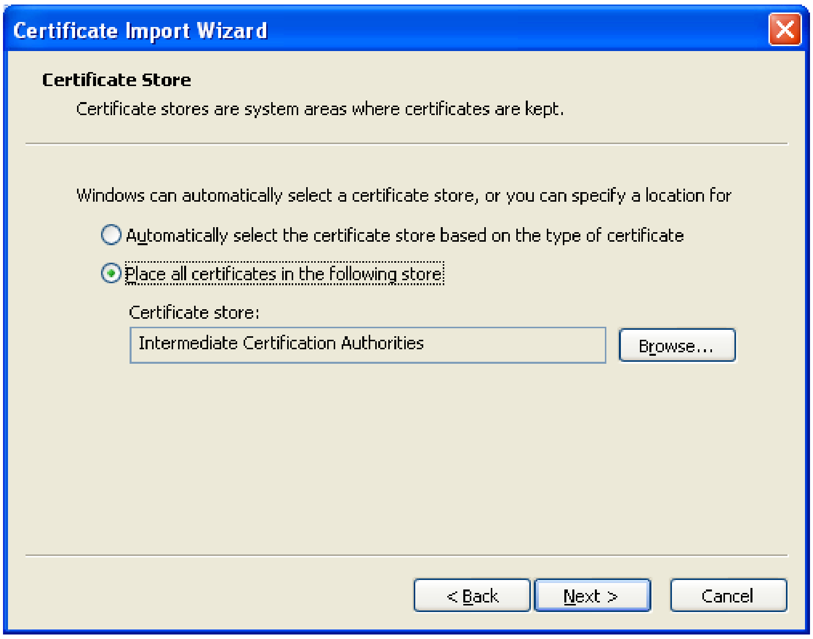
Note: More than one certificate can be stored in a single file in the following formats:

Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

8. Select a location to save the Certificate and click **Next**.



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for

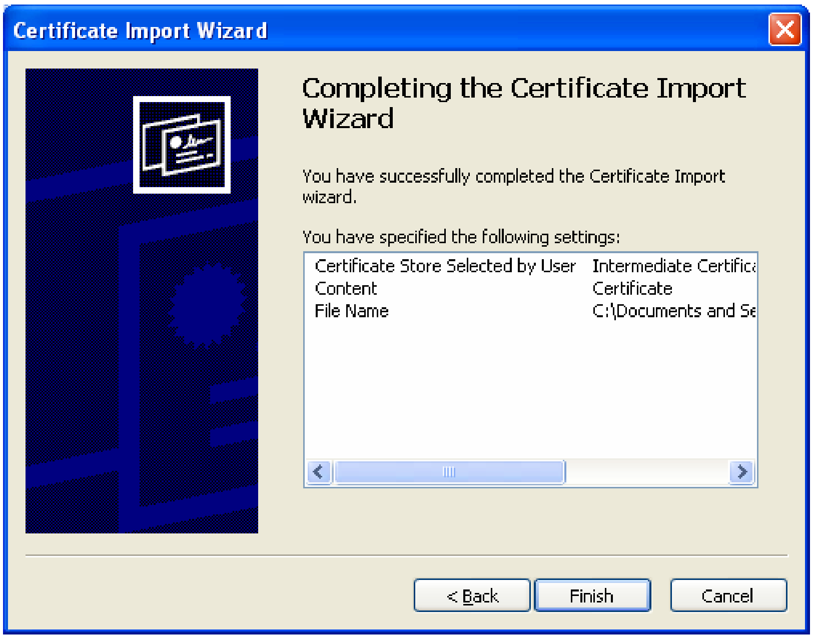
○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store:

Intermediate Certification Authorities

9. Click **Finish** to complete Certificate import.



Completing the Certificate Import Wizard

You have successfully completed the Certificate Import wizard.

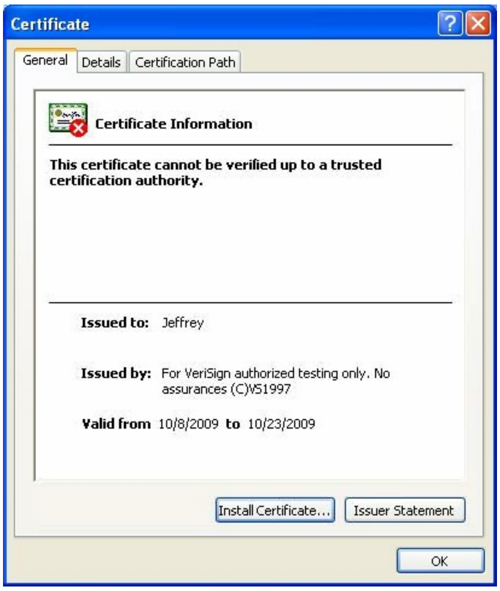
You have specified the following settings:

Certificate Store Selected by User	Intermediate Certific
Content	Certificate
File Name	C:\Documents and Se

The way to tell a secure web connection from unsafe one is by looking up a lock symbol (🔒) on your browser (on the bottom-right of browser of IE6 or on the address bar of IE7). You can double click on the symbol to examine the detail information of server side certificate.

Once you have prepared a publicly signed CA suite files, complete CA files upload in SSL Certificate page. A system reboot will make IP KVM to take the new CA suites as its certificate. You can verify the new certificate by looking into IP KVM certificate in next https session.

The following example demonstrates a publicly signed certificate and information registered to certificate authority (VeriSign).



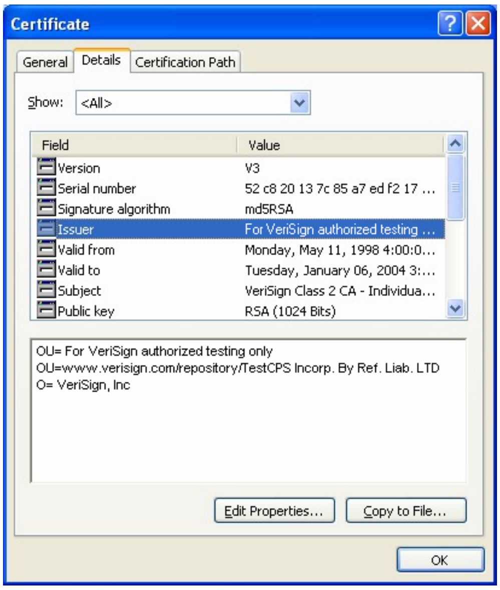
Certificate Information

This certificate cannot be verified up to a trusted certification authority.

Issued to: Jeffrey

Issued by: For VeriSign authorized testing only. No assurances (C)VS1997

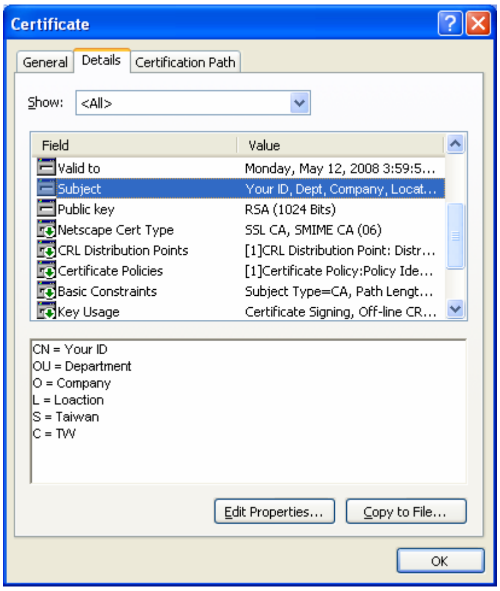
Valid from 10/8/2009 to 10/23/2009



Show: <All>

Field	Value
Version	V3
Serial number	52 c8 20 13 7c 85 a7 ed f2 17 ...
Signature algorithm	md5RSA
Issuer	For VeriSign authorized testing ...
Valid from	Monday, May 11, 1998 4:00:0...
Valid to	Tuesday, January 06, 2004 3:...
Subject	VeriSign Class 2 CA - Individua...
Public key	RSA (1024 Bits)

OU= For VeriSign authorized testing only
OU=www.verisign.com/repository/TestCPS Incorp. By Ref. Liab. LTD
O= VeriSign, Inc



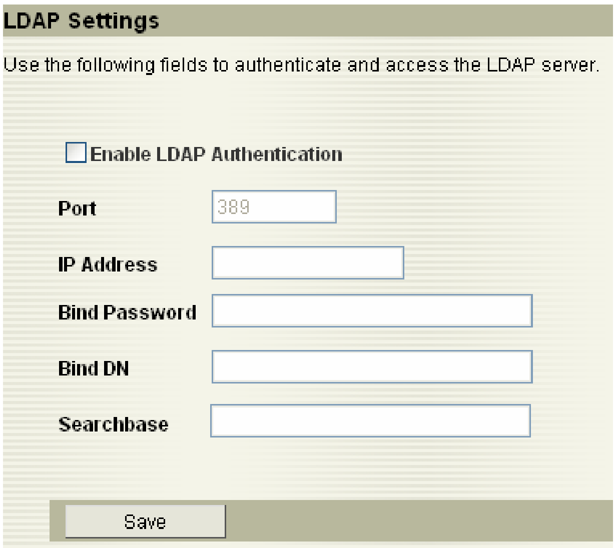
Show: <All>

Field	Value
Valid to	Monday, May 12, 2008 3:59:5...
Subject	Your ID, Dept, Company, Locat...
Public key	RSA (1024 Bits)
Netscape Cert Type	SSL CA, SMIME CA (06)
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Certificate Policies	[1]Certificate Policy:Policy Ide...
Basic Constraints	Subject Type=CA, Path Lengt...
Key Usage	Certificate Signing, Off-line CR...

CN = Your ID
OU = Department
O = Company
L = Loaction
S = Taiwan
C = TW

5.2.12 LDAP

This page helps you to download user list of LDAP (Lightweight Directory Access Protocol) server then create the user account from this list directly. LDAP is an application protocol for querying and modifying directory services running over TCP/IP.



LDAP Settings

Use the following fields to authenticate and access the LDAP server.

☐ Enable LDAP Authentication

Port: 389

IP Address:

Bind Password:

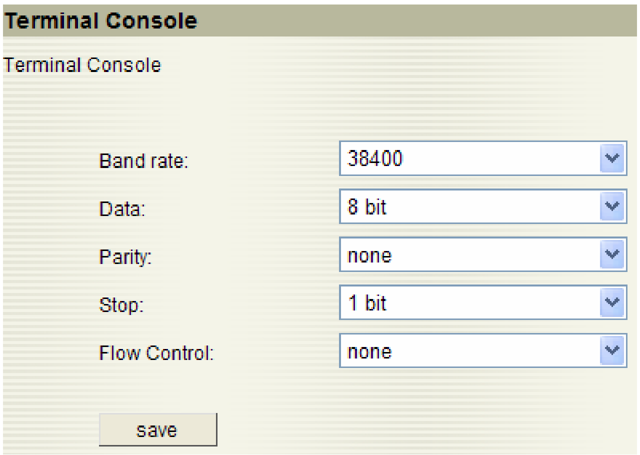
Bind DN:

Searchbase:

Item	Description
Enable LDAP Authentication	Check to enable LDAP authentication.
Port	Enter the port number of LDAP Server.
IP Address	Enter the IP address of LDAP Server.
Bind Password	Enter the password for authentication.
Bind DN	Enter the DN (Distinguished Name) for the server uses to bind to the directory.
Searchbase	Define the location in the directory from which the LDAP search begins

5.2.13 Terminal Console

This page allows you to configure the terminal console setting.



Terminal Console

Terminal Console

Band rate: 38400

Data: 8 bit

Parity: none

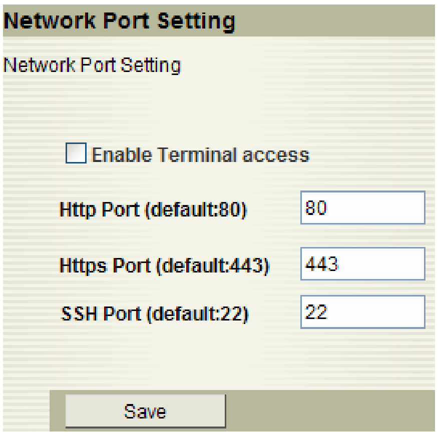
Stop: 1 bit

Flow Control: none

Item	Description
Band Rate	Select the bps (bits per second) from the drop-down list.
Data	Select the data bits from the drop-down list.
Parity	Select the parity type from the drop-down list.
Stop	Select the stop bits from the drop-down list.
Flow Control	Select the flow control method from the drop-down list.

5.2.14 Network Port Setting

This page allows you to configure network port settings.



Network Port Setting

Network Port Setting

☐ Enable Terminal access

Http Port (default:80) 80

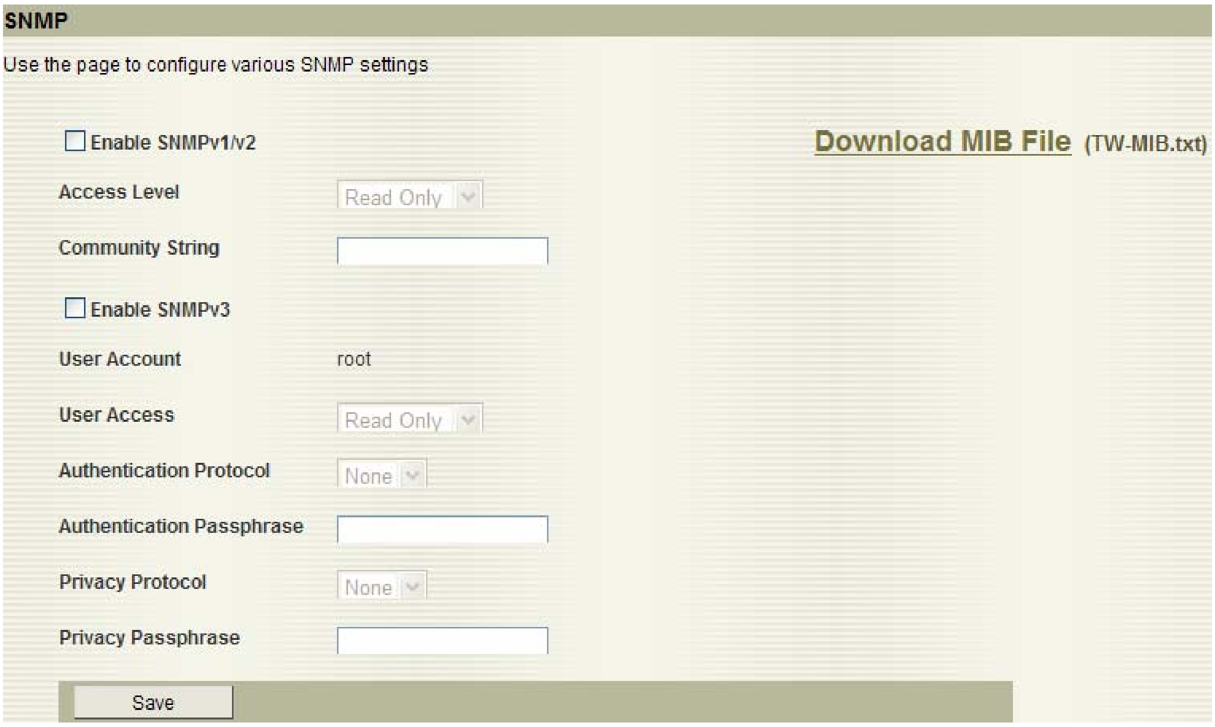
Https Port (default:443) 443

SSH Port (default:22) 22

Item	Description
Enable Terminal Access	Check to enable terminal access.
HTTP Port	Enter the HTTP (Hypertext Transfer Protocol) port number for network settings.
HTTPS Port	Enter the HTTPS (Hypertext Transfer Protocol Secure) port number for network settings.
SSH Port	Enter the SSH (Secure Shell) port number for network settings.

5.2.15 SNMP

This page allows you to configure SNMP (Simple Network Management Protocol) settings.



SNMP

Use the page to configure various SNMP settings

☐ Enable SNMPv1/v2

Download MIB File (TW-MIB.txt)

Access Level	Read Only
Community String	

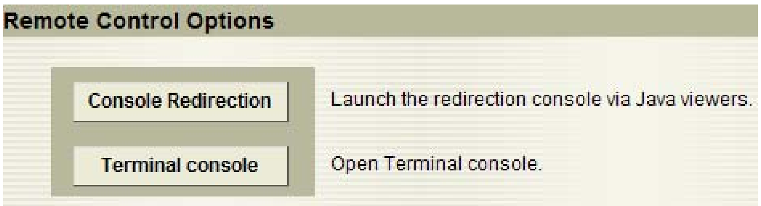
☐ Enable SNMPv3

User Account	root
User Access	Read Only
Authentication Protocol	None
Authentication Passphrase	
Privacy Protocol	None
Privacy Passphrase	

Item	Description
Enable SNMPv1/v2	Check to enable SNMPv1/v2.
Access Level	Select the access level to be read-and-write or read only.
Community String	Enter the community string (password) for the access.
Enable SNMPv3	Check to enable SNMPv3.
User Account	The account you login to the IP KVM.
User Access	Select the access level to be read-and-write or read only.
Authentication Protocol	Select the authentication protocol to be SHA (Secure Hash Algorithm), MD5 (Message-Digest algorithm 5) or None.
Authentication Passphrase	Enter the passphrase (password) for authentication.
Privacy Protocol	Select the privacy protocol to be DES (Data Encryption Standard (64-bit encryption)), AES (Advanced Encryption Standard (128-bit encryption)) or None.
Privacy Passphrase	Enter the passphrase (password) for authentication.

5.3 Remote Control

This page allows you to launch the redirection console or open the terminal console. The most powerful feature of IP KVM is the ability to redirect the host system's console. You can manage your host system as if it were physically in front of you.



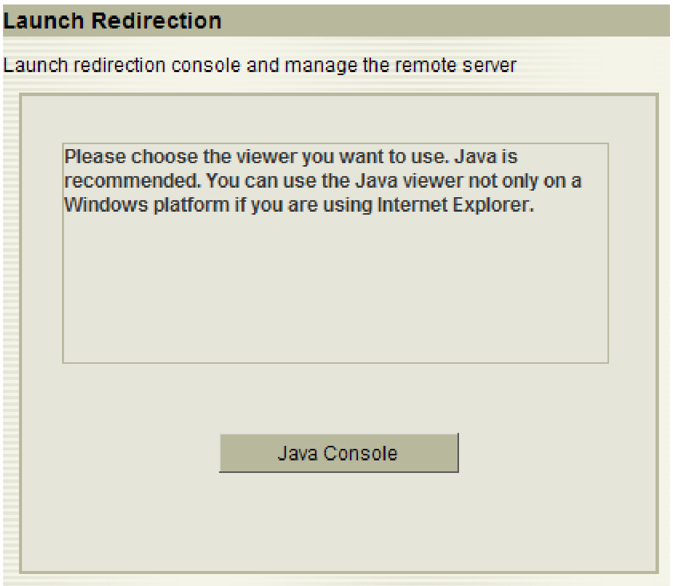
Remote Control Options

Launch the redirection console via Java viewers.

Open Terminal console.

5.3.1 Console Redirection

The most powerful feature of this IP KVM is the ability to redirect the host system's console. It means you can manage your host system as if it were physically in front of you, but not. This page allows you to start JAVA Remote Console (RC) session with the host system.



Launch Redirection

Launch redirection console and manage the remote server

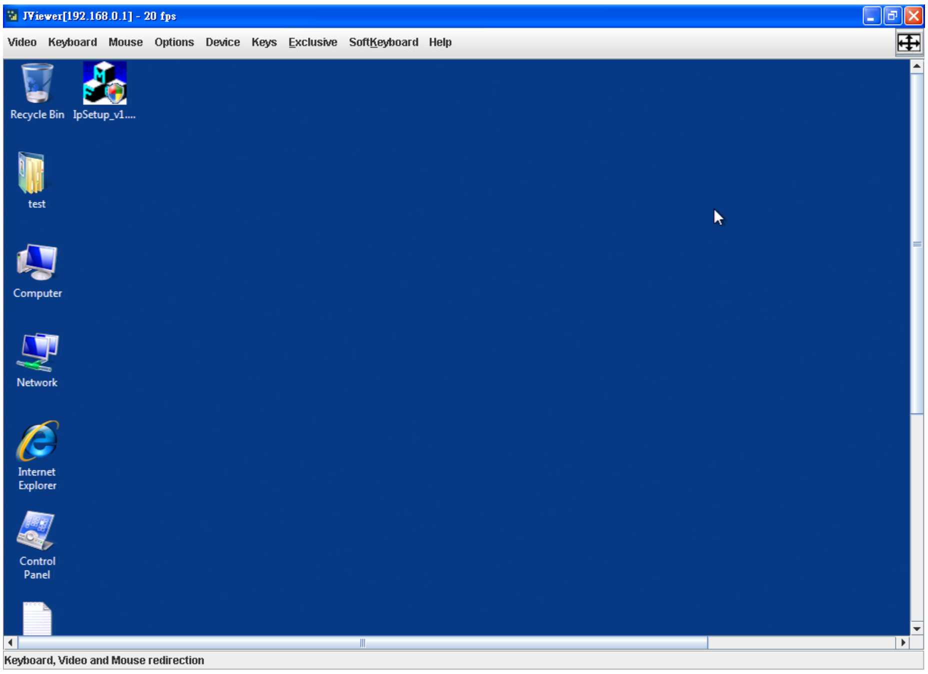
Please choose the viewer you want to use. Java is recommended. You can use the Java viewer not only on a Windows platform if you are using Internet Explorer.

1. Click **Java Console.** It will invoke the remote KVM redirection software, Java applet.

Note: In order to run this function, the system need support J2RE (Java 2 Runtime Environment) 1.6 and above or Sun JRE (Java Runtime Environment) 6.0 and above. You can get the Java Software from the website http://www.java.com/en/download.

Note: For the Remote Console function, the following TCP ports will be used: **443, 7578** and **12150**. So the network settings (e.g., IP filter of the IP KVM switch, the firewall) shall not block these TCP ports.

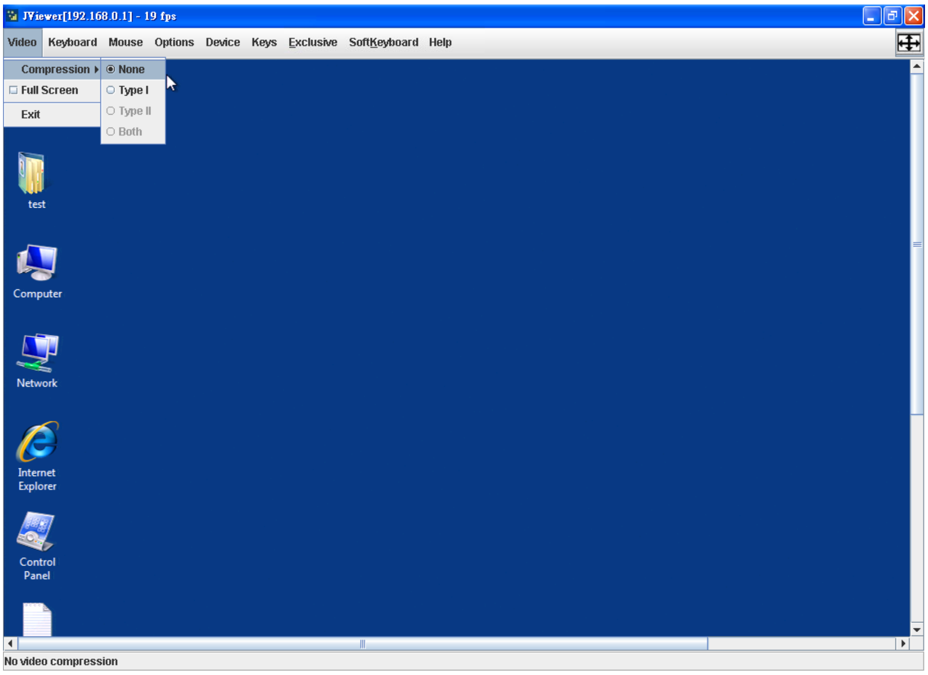
2. Click **OK** on the Security Warning. The remote console will display as below.



Keyboard, Video and Mouse redirection

5.3.1.1 Video

It allows you to configure the **Video** settings of remote console.

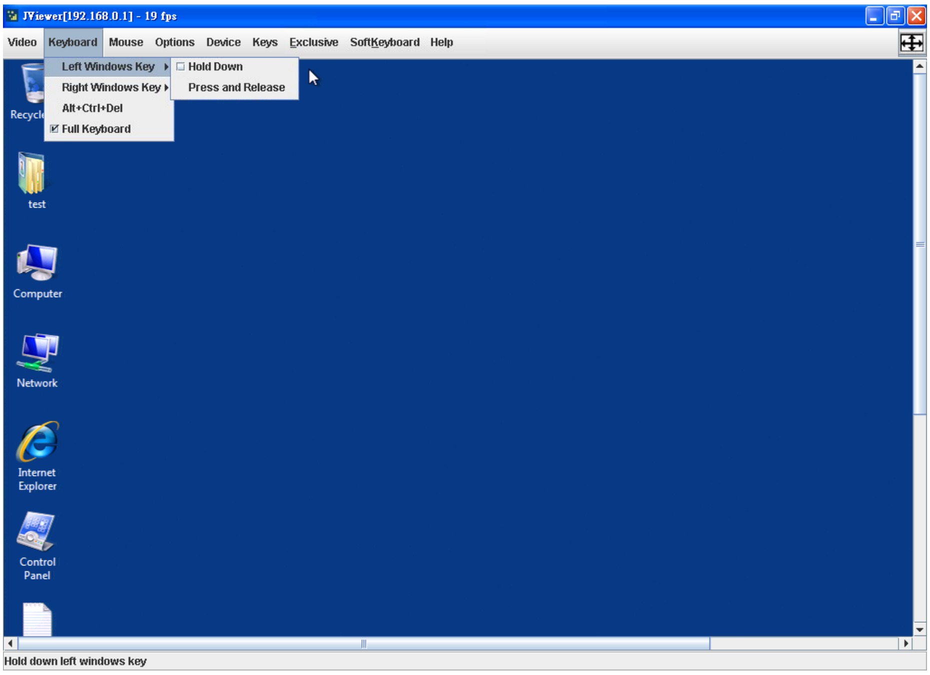


No video compression

Compression	This item is use to select the mode for compress video signal: ♦ None: (default) Use hardware compressing engine. For wide bandwidth internet. ♦ Type-I: Level 1 software compressing engine. For xDSL/Cable Modem.
Full Screen	This menu item can be used to view the *Console Redirection* in *Full Screen* mode. Note that you have to set your client system's screen resolution to 1280 x 1024 so that you can view the host system in true full screen.

5.3.1.2 Keyboard

It allows you to configure the **Keyboard** settings of remote console.

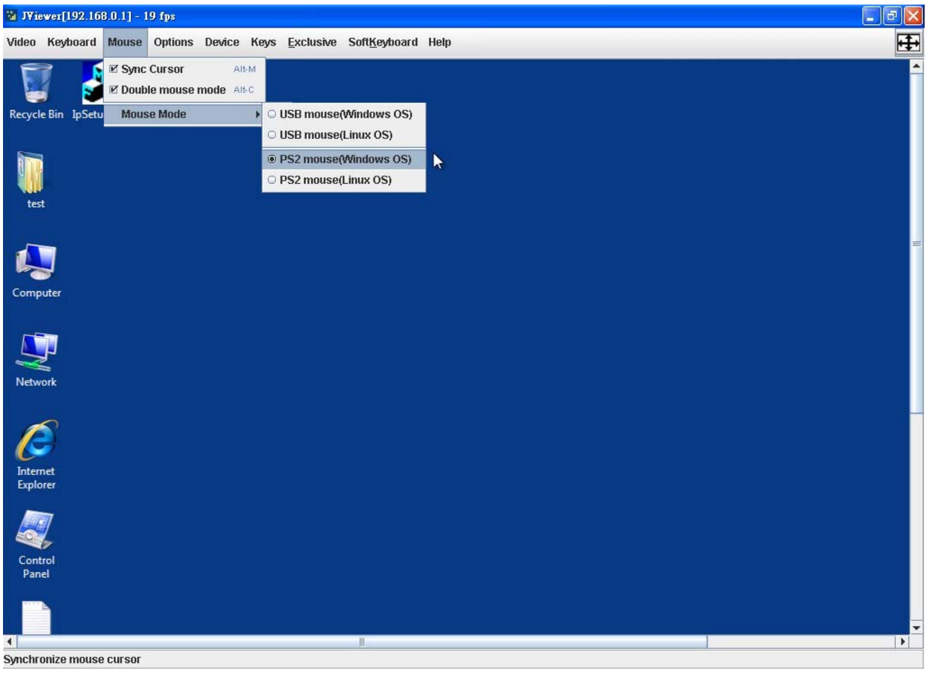


Hold down left windows key

Left Windows Key	This item is used to access the left-side <WINDOWS> key during a Console Redirection session. The following actions can be performed: - *Hold Down - Press and Release*
Right Windows Key	This item is used to access the right-side <WINDOWS> key during a Console Redirection session. The following actions can be performed: - *Hold Down - Press and Release*
Alt+Ctrl+Del	This item is used to act as if you press the <CTRL>, <ALT> and <DEL> keys down simultaneously on the host system that you are redirecting.
Full Keyboard	This item is used to enable all keystroke of your keyboard.

5.3.1.3 Mouse

It allows you to configure the **Mouse** settings of remote console.

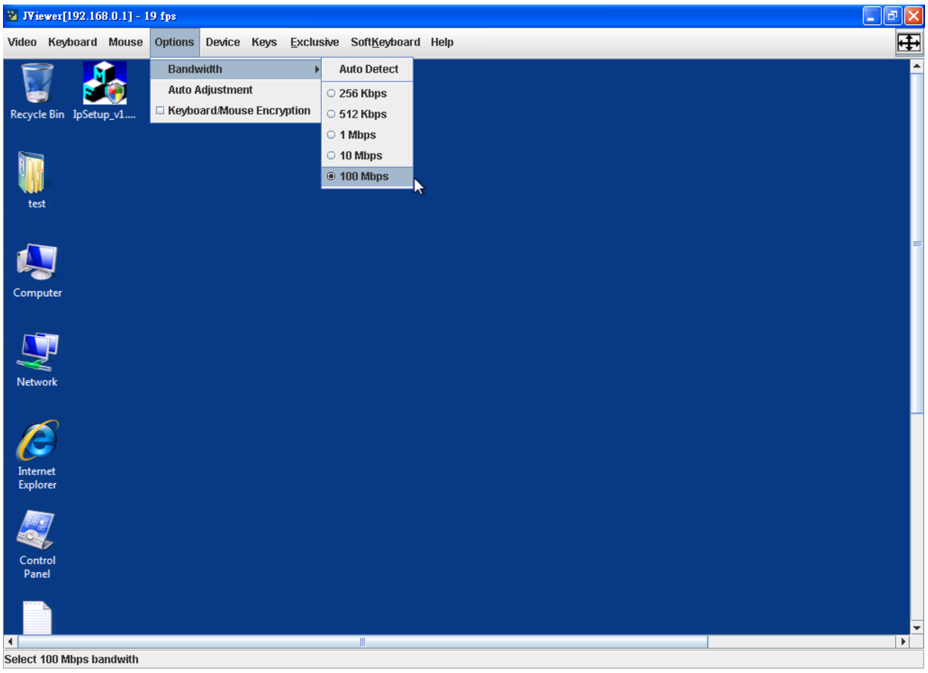


Synchronize mouse cursor

Sync Cursor	Select this function to bring the mouse cursor in or out of remote console.
Double Mouse Mode	Select this function to enable double mouse mode.
Mouse Mode	Select the mouse mode of remote console.

5.3.1.4 Options

It allows you to configure bandwidth, auto-adjust the screen’s position and enable Keyboard/Mouse Encryption of remote console.

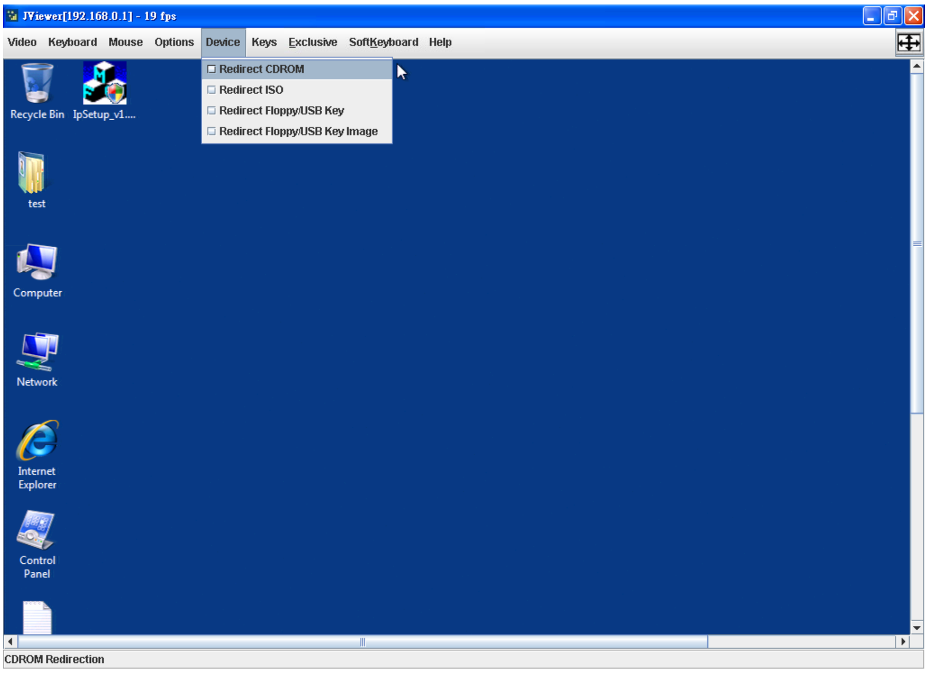


Select 100 Mbps bandwidth

Bandwidth	To regulate the network bandwidth.
Auto Adjustment	To auto adjust the position of Java Viewer on the screen.
Keyboard/ Mouse Encryption	To encrypt the keyboard/mouse signal

5.3.1.5 Device (Virtual Media Redirection)

With Redirection function you can work with a drive from your local computer on the remote machine. The drive is hereby shared over a TCP network connection. Devices such as floppy drives, CD-ROMs and other removable devices like USB sticks can be redirected.

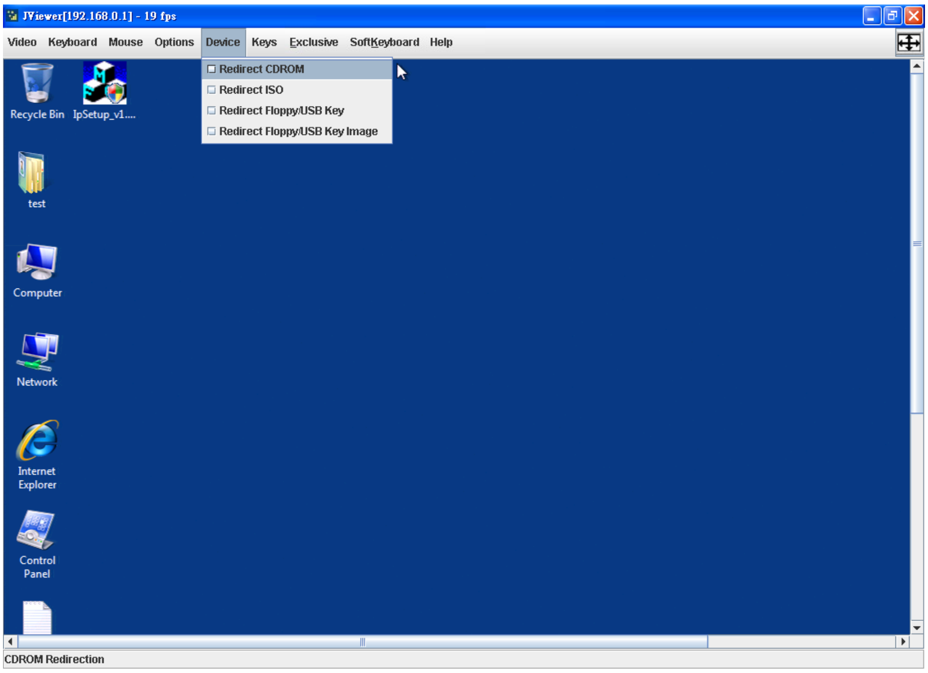


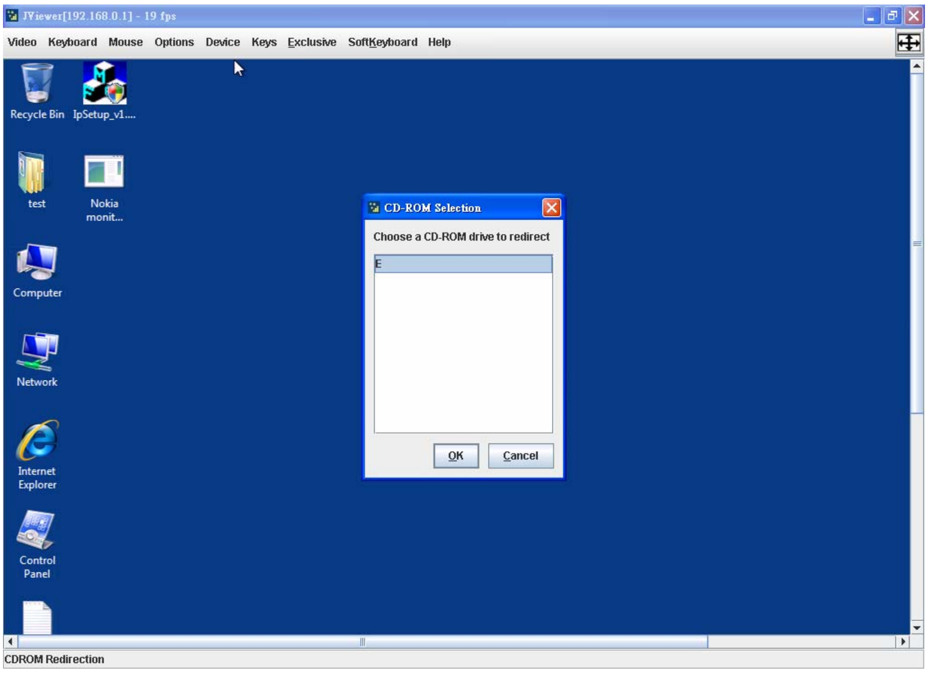
Redirect CDROM	This menu item can be used to start or stop the redirection of the CD-ROM drive.
Redirect ISO	It can redirect the CD Image file from client computer.
Redirect Floppy/ USB Key	This menu item can be used to start or stop the redirection of the floppy or USB drive.
Redirect Floppy/ USB Key Image	It can be chose the Floppy or USB Image file from client computer.

Please note that Drive Redirection works on a level which is far below the operating system. That means that neither the local nor the remote operating system is aware that the drive is currently redirected, actually. This may lead to inconsistent data as soon as one of the operating systems (either from the local machine, or from the remote host) is writing data on the device. If write support is enabled the remote computer might damage the data and the file system on the redirected device. On the other hand, if the local operating system writes data to the redirected device the drive cache of the operating system of the remote host might contain older data. This may confuse the remote host’s operating system. It is recommended to use the Drive Redirection with care.

The following example is the operating procedures of CD-ROM redirection.

1. Make sure the USB cable is connected between IP KVM unit and host computer.
2. Select **Device > Redirect CDROM**.
3. Choose a drive to be redirected (e.g., drive E of local computer).

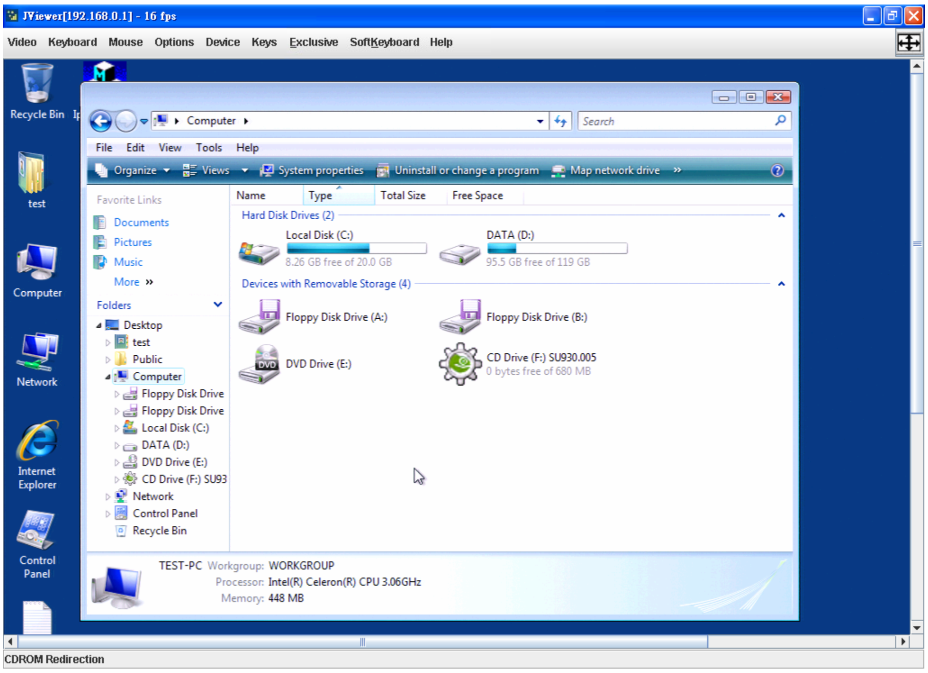

JViewer[192.168.0.1] - 19 fps
Video Keyboard Mouse Options Device Keys Exclusive SoftKeyboard Help
☐ Redirect CDROM
☐ Redirect ISO
☐ Redirect Floppy/USB Key
☐ Redirect Floppy/USB Key Image
Recycle Bin
IpSetup_v1....
test
Computer
Network
Internet Explorer
Control Panel
CDROM Redirection



Choose a CD-ROM drive to redirect

E

4. Open the redirected drive (e.g., drive **E**, which is redirected to drive E of local computer).



5. Inspect the redirected contents of drive E (local computer) and drive G (host computer) should be the same.

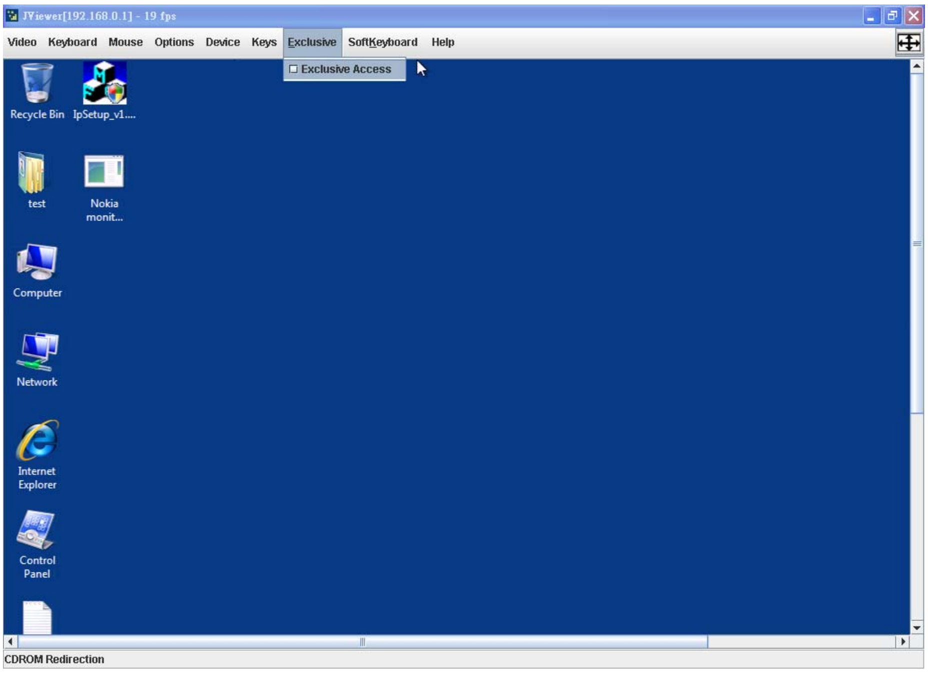
5.3.1.6 Keys (Remote Button Key)

Remote Botton Key allows you to specify a hotkey combination which starts either the mouse synchronization process if pressed in the Remote Console, or is used to leave the single mouse mode.

Remote Console Button Keys	Button Keys allow simulating keystroes on the remote system that cannot be generated locally. The reason for this might be a missing key or the fact, that the local operating system of the Remote Console is unconditionally catching this keystroke already. Typical examples are “Control+Alt+Delete” on Windows and DOS, what is always caught, or “Control+Backspace” on Unix or Unix-like OS for terminating the X-Server. The syntax to define a new Button Key is as follows: **[confirm] <keycode>[+|-[*]<keycode>]*** “confirm” requests confirmation by a dialog box before the key strokes will be sent to the remote host. “keycode” is the key to be sent. Multiple key codes can be concatenated with a plus, or a minus sign. The plus sign builds key combinations, all keys will be pressed until a minus sign or the end of the combination is encountered. In this case all pressed keys should be released in reversed sequence. The minus sign builds single, separate key presses and releases. The star inserts a pause with duration of 100 milliseconds.

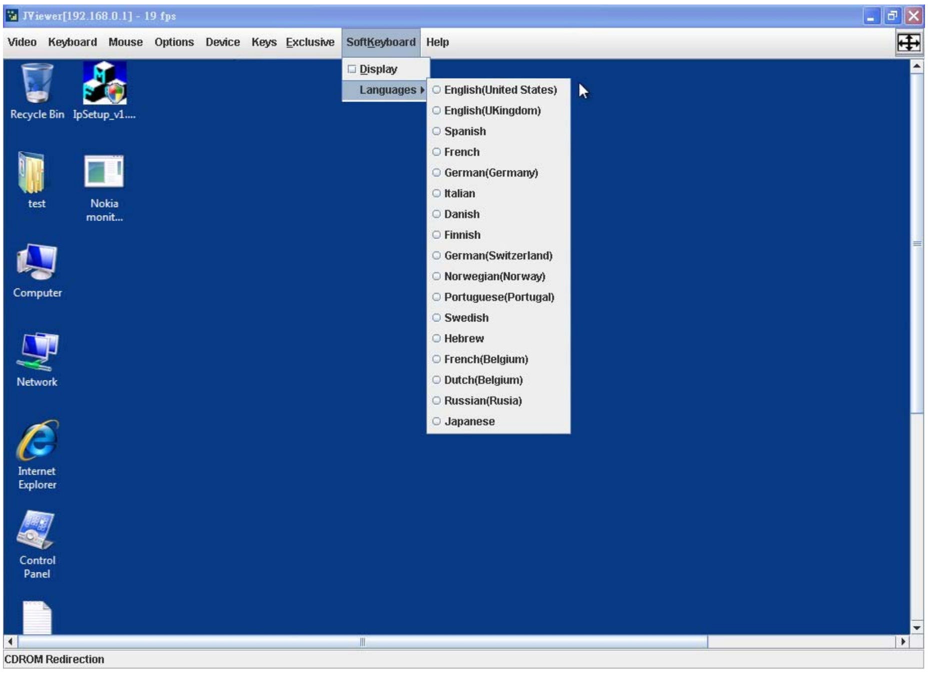
5.3.1.7 Exclusive

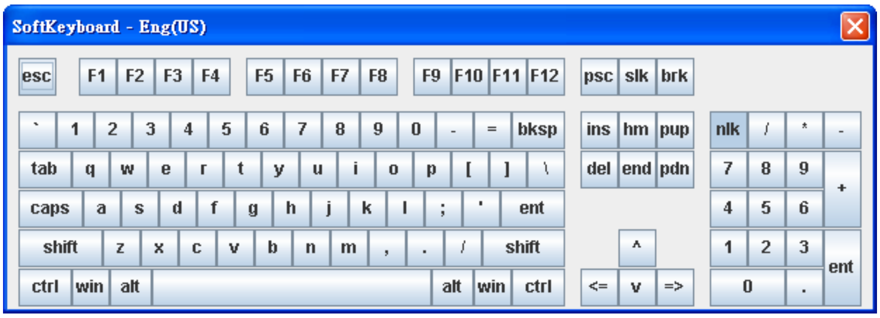
Enable Exclusive to force all other users to exit from the Remote Consoles. No one can open the Remote Console at the same time until this user disables the exclusive access or logs off.



5.3.1.8 Soft Keyboard

A soft keyboard (also called an on-screen keyboard or software keyboard) is a system that replaces the hardware keyboard on a computing device with an on-screen image map. It enables you to do any input as you were using a hardware keyboard.

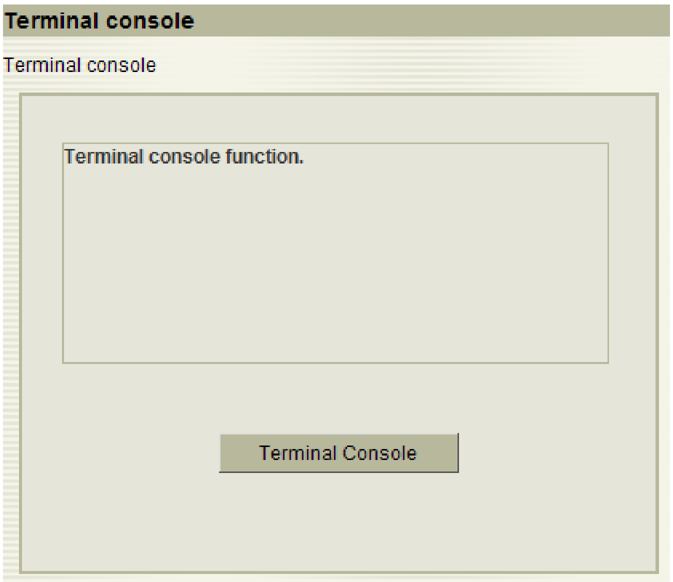



SoftKeyboard - Eng(US)
esc F1 F2 F3 F4 F5 F6 F7 F8 F9 F10 F11 F12 psc slk brk
` 1 2 3 4 5 6 7 8 9 0 - = bksp ins hm pup nlk / * -
tab q w e r t y u i o p [ ] \ del end pdn 7 8 9 +
caps a s d f g h j k l ; ' ent 4 5 6
shift z x c v b n m , . / shift ^ 1 2 3 ent
ctrl win alt alt win ctrl <= v => 0 .

Display	Pops up the soft keyboard. The soft keyboard is necessary in case your host system runs a completely different language and country mapping than your administration machine.
Language	Used for choosing the specific language and country mapping of the soft keyboard.

5.3.2 Terminal Console

You must enable remote access on Network Port Settings page before you can use this function.

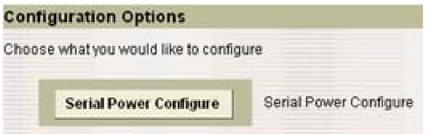

Terminal console

Terminal console

Terminal console function.

5.4 Serial Power Control

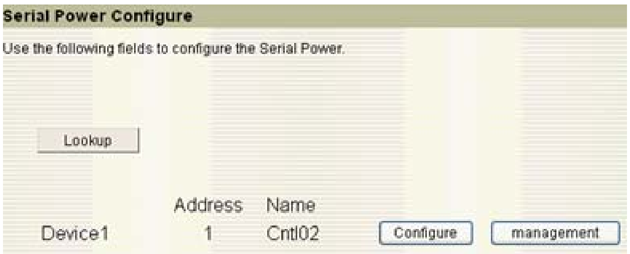
This page allows you to configure Serial Power application over LAN. Click **Serial Power Configure** to setup the settings of Serial Power.



Configuration Options

Choose what you would like to configure

Click **Lookup** to search the available Serial Power devices.

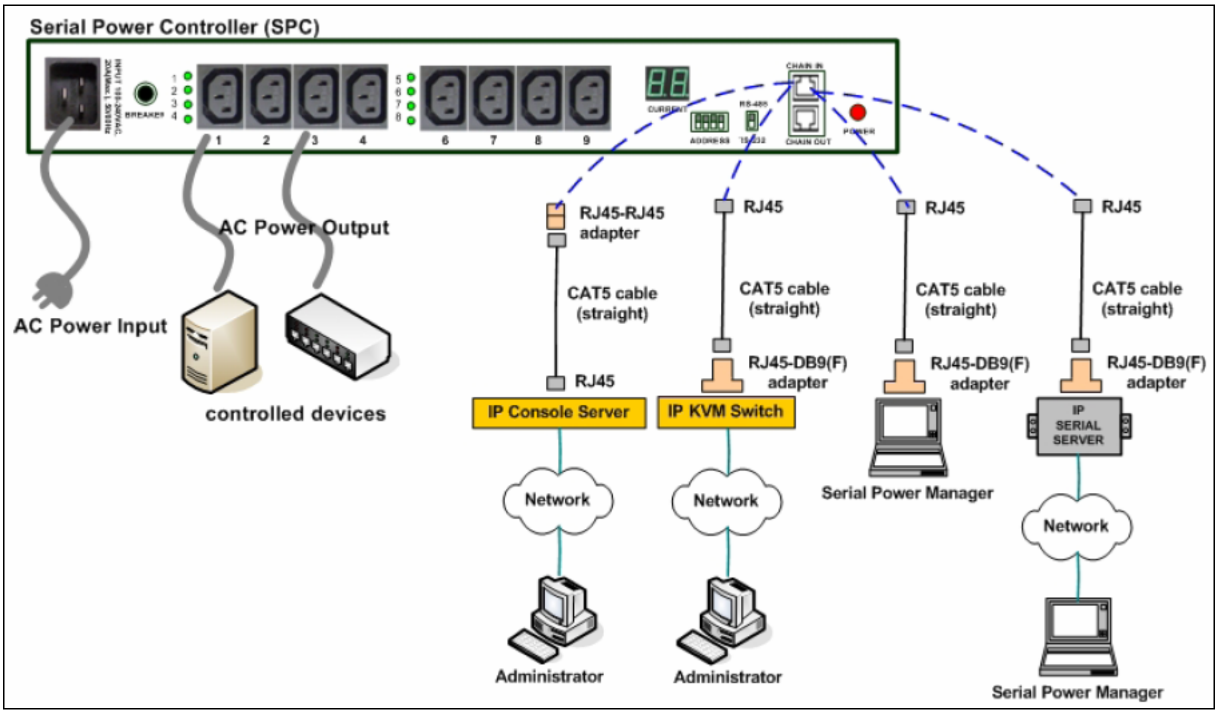


Serial Power Configure

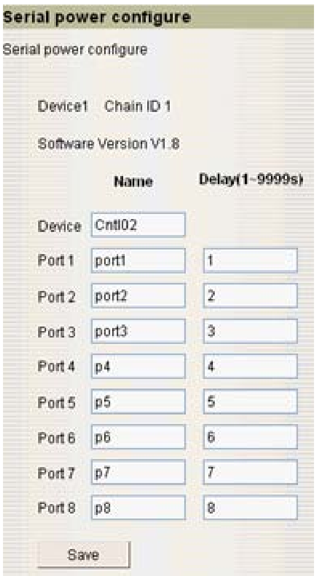
Use the following fields to configure the Serial Power.

	Address	Name		
Device1	1	Cntl02	Configure	management

The IP KVM offers Configuration page and Management sub-pages for SPC control. Below is an example diagram of SPC application. Please refer to Serial Power Controller's User Manual for mores details.



The Configuration page allows you to configure or modify the name and delay time of each port.



Serial power configure

Serial power configure

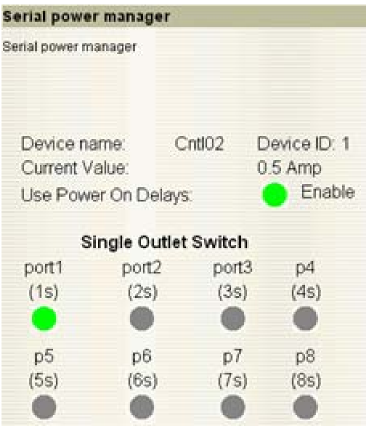
Device1 Chain ID 1

Software Version V1.8

	Name	Delay(1~9999s)
Device	Cntl02	
Port 1	port1	1
Port 2	port2	2
Port 3	port3	3
Port 4	p4	4
Port 5	p5	5
Port 6	p6	6
Port 7	p7	7
Port 8	p8	8

Device /Port Name	Configure the device and each port name of the Serial Power.
Port Delay Time	Configure the delay time of each port from 1 to 9999 seconds.

The Management page provides multiple SPC control options for you to configure. With IP KVM networking capability, all the SPC management can be done remotely, anywhere and anytime.



Serial power manager

Serial power manager

Device name: Cntl02 Device ID: 1

Current Value: 0.5 Amp

Use Power On Delays: ● Enable

Single Outlet Switch

port1	port2	port3	p4
(1s)	(2s)	(3s)	(4s)
●	●	●	●
p5	p6	p7	p8
(5s)	(6s)	(7s)	(8s)
●	●	●	●

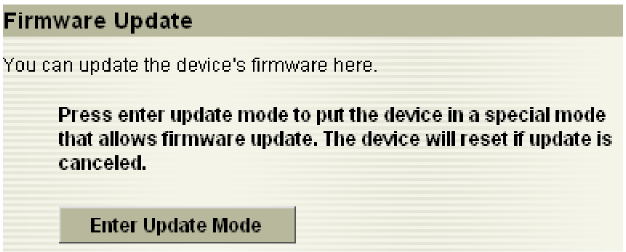
Current Value	Shows the current value of the serial power.
Use Power on Delays	Select to enable (green button) the delay time function of Serial Power.
Single Outlet Switch	Select to turn the switch of outlet On (green button) or Off (gray button) individually. It also shows the name and the delay time of the outlet. The outlet number depends on the Serial Power device you connected.

5.5 Maintenance

5.5.1 Firmware Update

Firmware can be easily upgraded via web page. This section describes the update procedures.

1. Select **Maintenance** from the Menu Bar.
2. Click **Enter Update Mode**.



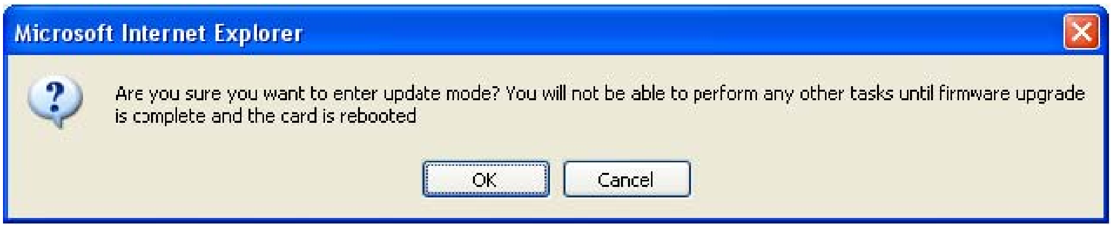
Firmware Update

You can update the device's firmware here.

Press enter update mode to put the device in a special mode that allows firmware update. The device will reset if update is canceled.

Note: Once enter this mode the device will reboot eventually.

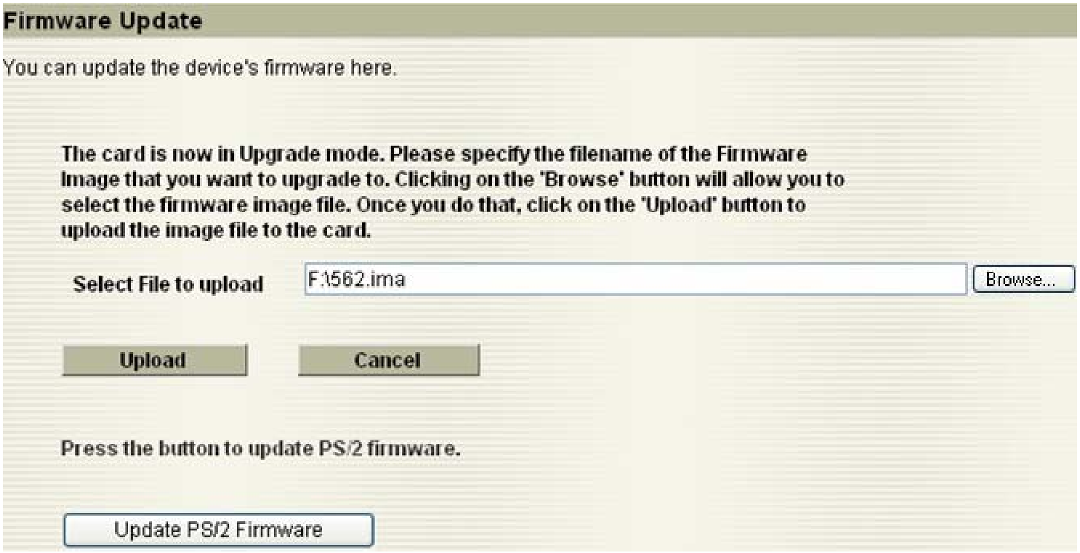
3. Click **OK**.



Microsoft Internet Explorer

Are you sure you want to enter update mode? You will not be able to perform any other tasks until firmware upgrade is complete and the card is rebooted

4. Click **Browse** and select the file of the firmware image that you want to upgrade to or click **Cancel** to exit from update mode.
5. Click **Upload** to upload the image file to the IP KVM.



Firmware Update

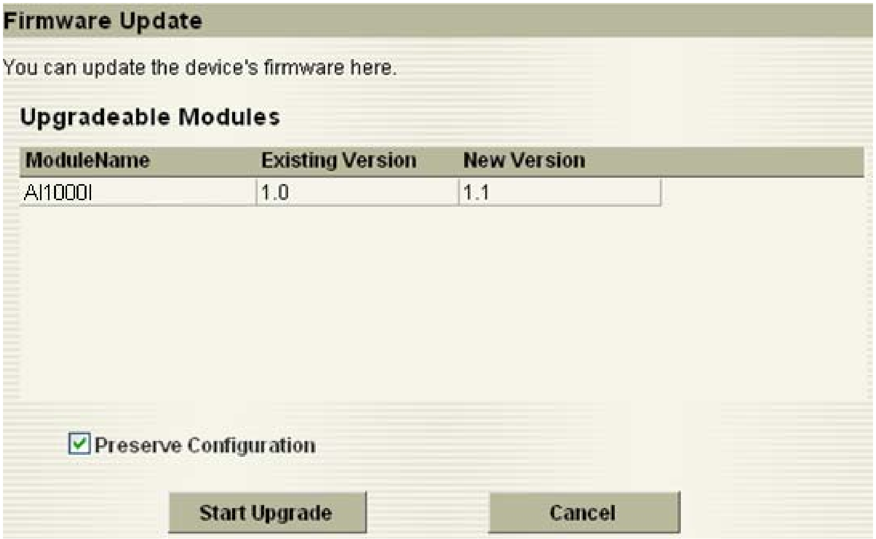
You can update the device's firmware here.

The card is now in Upgrade mode. Please specify the filename of the Firmware Image that you want to upgrade to. Clicking on the 'Browse' button will allow you to select the firmware image file. Once you do that, click on the 'Upload' button to upload the image file to the card.

Select File to upload F:\562.ima

Press the button to update PS/2 firmware.

6. Click **Start Upgrade**.



Firmware Update

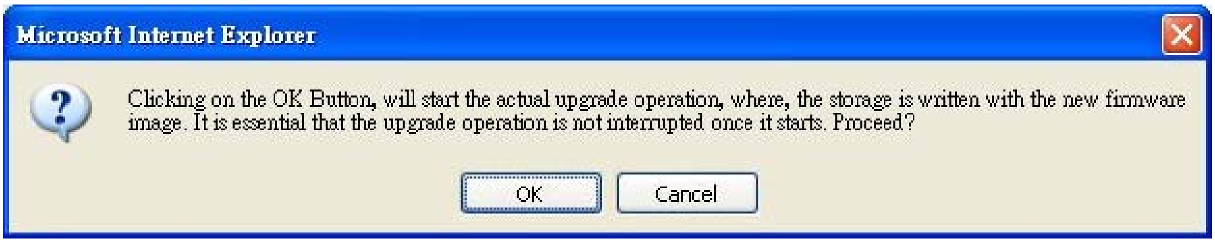
You can update the device's firmware here.

Upgradeable Modules

ModuleName	Existing Version	New Version
AI1000I	1.0	1.1

☑ Preserve Configuration

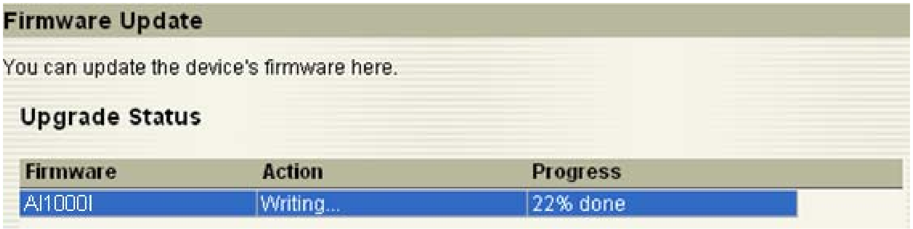
7. Click **OK.**



Microsoft Internet Explorer

Clicking on the OK Button, will start the actual upgrade operation, where, the storage is written with the new firmware image. It is essential that the upgrade operation is not interrupted once it starts. Proceed?

Warning!!! During this upgrading process, we should not disconnect the power or the Ethernet cable, since it may cause upgrade failure and destroy the image in Flash memory. In this case, we have to upgrade though bootloader process, which is not as friendly as the web method.



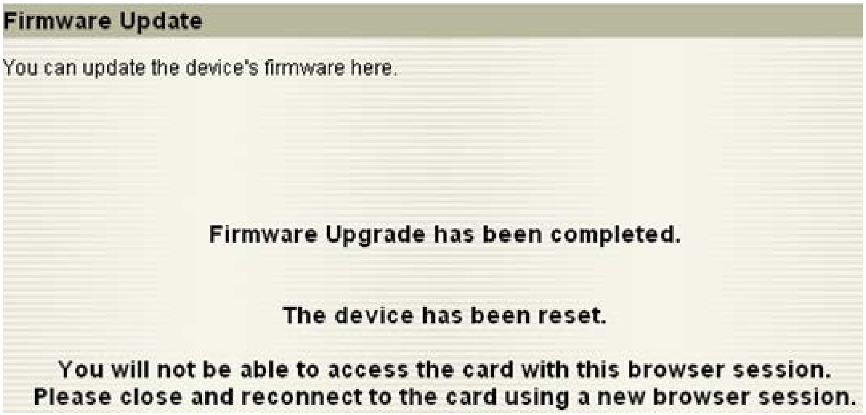
Firmware Update

You can update the device's firmware here.

Upgrade Status

Firmware	Action	Progress
AI1000I	Writing...	22% done

8. After a few seconds, the message **Firmware Upgrade has been completed** will be shown, indicating the new firmware has been upgraded into the Flash memory.



Firmware Update

You can update the device's firmware here.

Firmware Upgrade has been completed.

The device has been reset.

You will not be able to access the card with this browser session.
Please close and reconnect to the card using a new browser session.

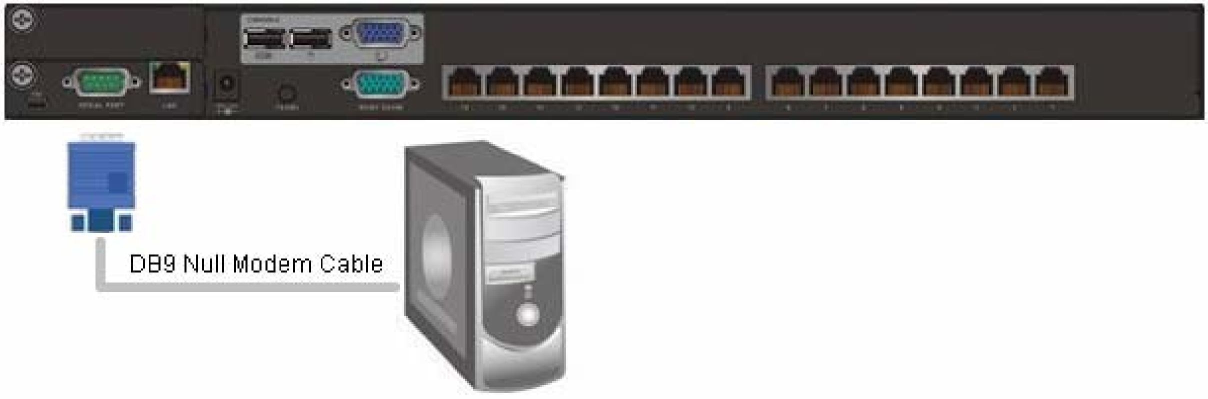
If you want to run the new firmware, you need to close and refresh the browser session. It will take about one minute to finish the system reboot.

Warning!!! DO NOT power off the IP KVM or disconnect Ethernet cable while upgrading process. This may cause upgrade failure and destroy the image in Flash memory.

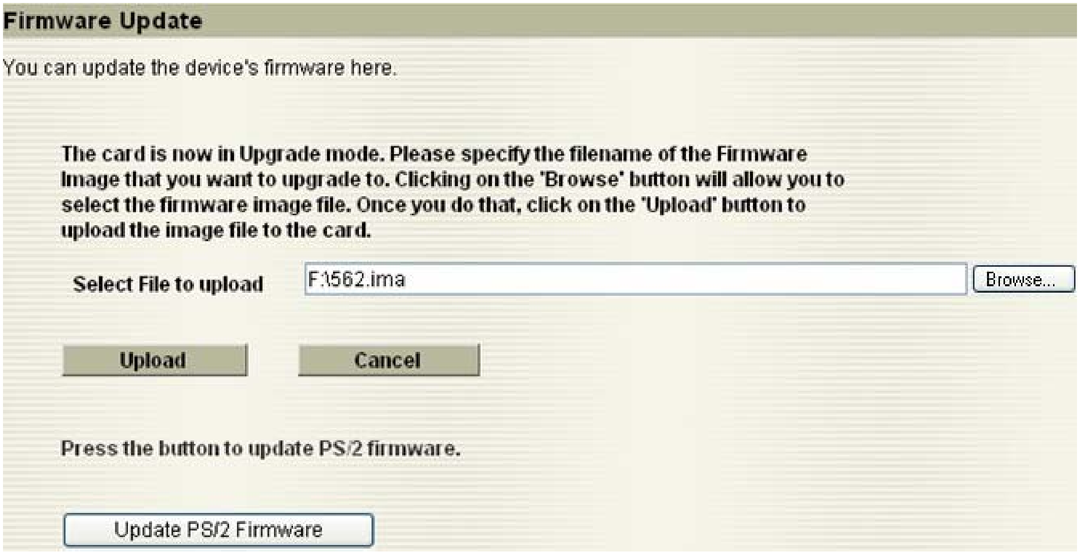
Warning!!! A new firmware release version may need one or two images to upgrade. **You have to upgrade all to-be upgraded images before rebooting the system.** Otherwise may cause inconsistency between kernel and application firmware and the system may not be able to start up successfully. In this case, we have to upgrade though bootloader process, which is not as friendly as the web method.

5.5.2 PS/2 Firmware Update

1. Refer to the diagram below. Connect the DB9 Serial Port on IP KVM to computer with a DB9 Null modem cable (not include in the package).



2. Login to the IP KVM. From **Maintenance** item then **Firmware Update**. Click **Update PS/2 Firmware** to update the image file to the IP KVM.



Firmware Update

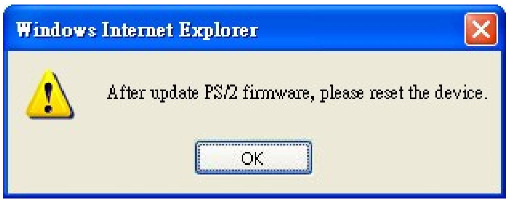
You can update the device's firmware here.

The card is now in Upgrade mode. Please specify the filename of the Firmware Image that you want to upgrade to. Clicking on the 'Browse' button will allow you to select the firmware image file. Once you do that, click on the 'Upload' button to upload the image file to the card.

Select File to upload: F:\562.ima

Press the button to update PS/2 firmware.

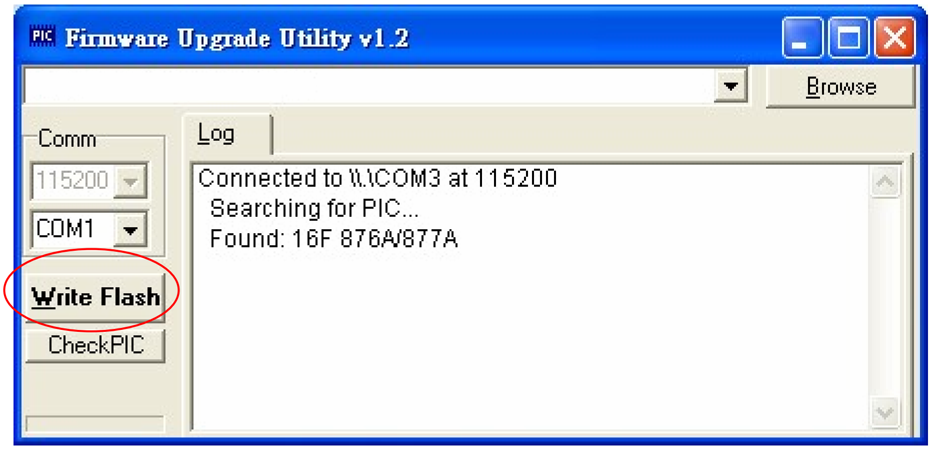
3. Click **OK**.



Windows Internet Explorer

After update PS/2 firmware, please reset the device.

4. Double click to launch “Firmware Upgrade Utility.exe”.
5. Click **CheckPIC** to search IP KVM. The message will then display when found the IP KVM.

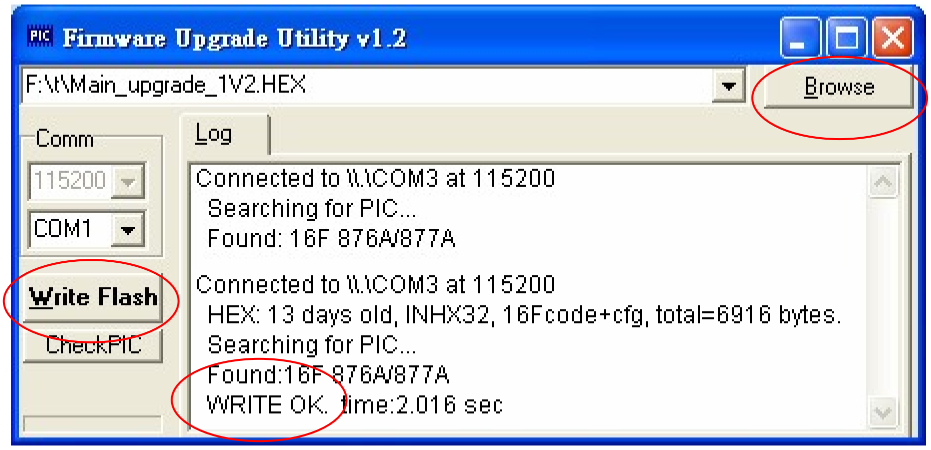


Firmware Upgrade Utility v1.2

```
Connected to \\.\COM3 at 115200
 Searching for PIC...
 Found: 16F 876A/877A
```

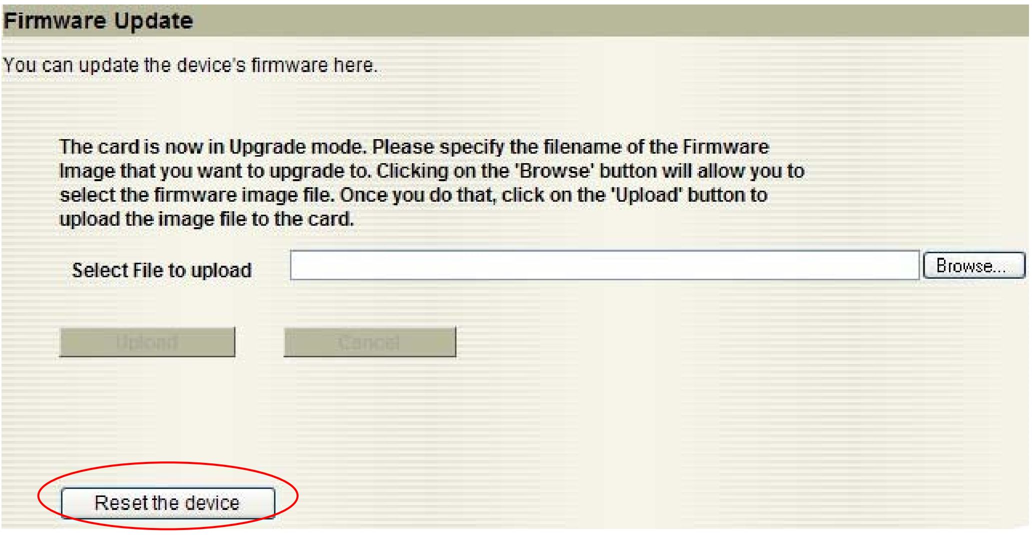
6. Click **Browse** to select the upgrade file. Make sure the file you select is the correct version for upgrading.
7. Click **Write Flash** to start to upgrade. The upgrade process takes about 2 seconds.

8. A “WRITE OK” message will then display when the upgrade process is completed successfully.



```
Connected to \\.\COM3 at 115200
 Searching for PIC...
 Found: 16F 876A/877A

Connected to \\.\COM3 at 115200
 HEX: 13 days old, INHX32, 16Fcode+cfg, total=6916 bytes.
 Searching for PIC...
 Found:16F 876A/877A
 WRITE OK.  time:2.016 sec
```

9. Click the **Reset the device**.

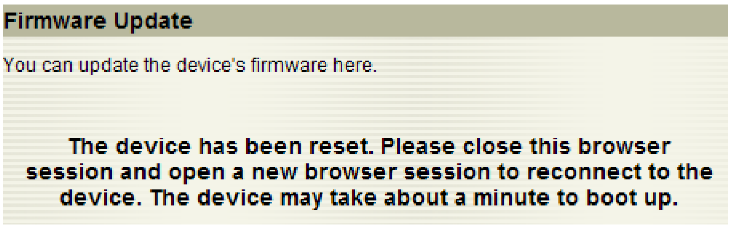


Firmware Update

You can update the device's firmware here.

The card is now in Upgrade mode. Please specify the filename of the Firmware Image that you want to upgrade to. Clicking on the 'Browse' button will allow you to select the firmware image file. Once you do that, click on the 'Upload' button to upload the image file to the card.

10. The device will be reset. Please close the browser session and re-open a new one to reconnect to the IP KVM.



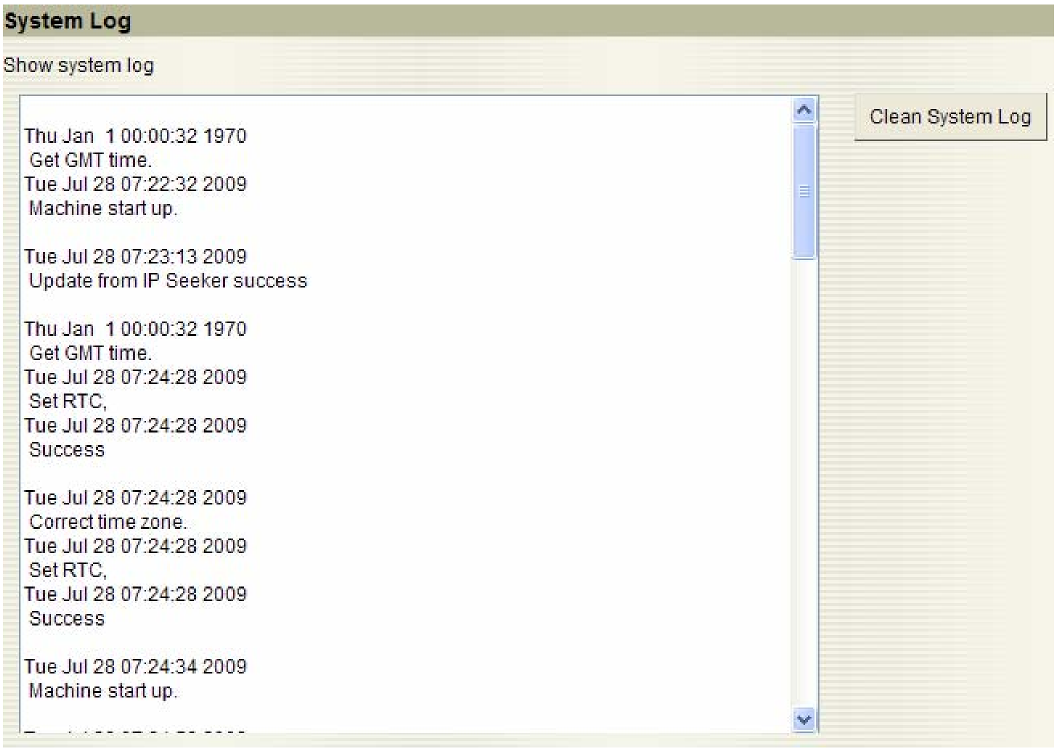
Firmware Update

You can update the device's firmware here.

The device has been reset. Please close this browser session and open a new browser session to reconnect to the device. The device may take about a minute to boot up.

5.6 System Log

The log function will log the system operation, such as login activity, no matter fail or success information. The system log buffer is pre-allocated at 300K bytes size. If the logging data exceeds the pre-allocated size, the new data will overwrite the old logs.



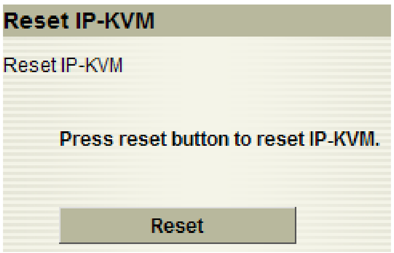
System Log

Show system log

```
Thu Jan  1 00:00:32 1970
 Get GMT time.
Tue Jul 28 07:22:32 2009
 Machine start up.

Tue Jul 28 07:23:13 2009
 Update from IP Seeker success

Thu Jan  1 00:00:32 1970
 Get GMT time.
Tue Jul 28 07:24:28 2009
 Set RTC,
Tue Jul 28 07:24:28 2009
 Success

Tue Jul 28 07:24:28 2009
 Correct time zone.
Tue Jul 28 07:24:28 2009
 Set RTC,
Tue Jul 28 07:24:28 2009
 Success

Tue Jul 28 07:24:34 2009
 Machine start up.
```

5.7 Reset IP KVM

The page allows you to reset IP KVM by pressing the Reset button.



Reset IP-KVM

Reset IP-KVM

Press reset button to reset IP-KVM.

6 Troubleshooting

Make sure that all cables are well seated. Label all cables with the name/number for each respective computer to avoid confusion.

1. The KVM Switch’s LED does not light up.
   - ♦ Make sure the power adapter is plugged into KVM Switch. If the LED still won’t light up, perform soft reset (press the reset button on KVM Switch’s front panel) to reset KVM Switch.
   - ♦ Power cycle KVM Switch.

2. The computer has started up, but keyboard or mouse does not work.
   - ♦ Make sure your keyboard and mouse work fine if directly plugged into the computer.
   - ♦ PS/2 computer’s keyboard and mouse are not hot pluggable, make sure PS/2 cable are well connected then reboot the computer.
   - ♦ Make sure USB cables are well connected then reboot the computer.
   - ♦ Do not press any key on the keyboard while the selected computer is booting up. Otherwise it might cause the keyboard error or keyboard detection fail by the Host side.
   - ♦ Try a different keyboard, but use only 101/102/104-key keyboard.
   - ♦ Do not move the mouse or press the mouse buttons when switching ports.
   - ♦ Power cycle KVM Switch.

3. No video signal is displayed on the monitor.
   - ♦ Connect your monitor directly to the server to verify that your monitor is functioning properly.
   - ♦ Make sure all connectors are connected properly.
   - ♦ Make sure the power adapter is connected to the KVM Switch.
   - ♦ Use hotkey "SPACE" to bring up the OSD, and confirm the port is selected and connected to a server.
   - ♦ See next item, make sure the computer’s VGA output resolution match the monitor’s resolution.

4. The computer’s VGA resolution does not match the monitor’s resolution.
    - Make sure VGA resolution works fine if directly connect the monitor to the computer.
    - Turn off the computer, wait few seconds then turn it on again. Note that during computer startup, it will try to obtain the information of the connected monitor’s resolution from its VGA port. So before computer startup, the monitor and KVM Switch should be already ON and running.
    - The DDC function of KVM Switch will dynamically detect and copy the DDC data from the monitor that attached to the LOCAL console port, and that data will be fed to the host computer during computer startup.
    - When you want to change the monitor, power off the KVM Switch first. Then connect the new monitor to the KVM Switch and power on the monitor. You must power the monitor before KVM Switch, so that the KVM Switch can detect the monitor’s settings and pass the settings to the computer.
    - The recommended power on sequence is: monitor → KVM Switch → the computers.

5. I forgot the password for login to OSD.
    - Try the default password eight zeros “00000000”.
    - If you forget the password you changed, please contact your supplier.

Appendix A: Specifications

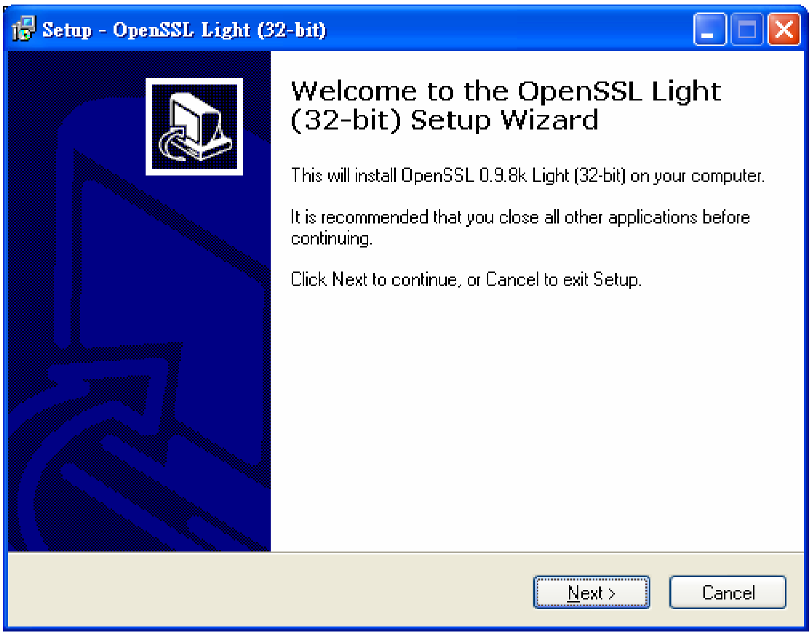
Connector	LAN: Standard RJ-45 Connector Serial Port: DB9 (male) Mini USB: USB 2.0 Type B
OS Supported	Windows 2000/XP/Vista/Server 2003, Linux Fedora core 6.0 (or above)
Browser Supported	IE6.0, Firefox 1.0 (or above)
Video Resolution (Local Console)	1920x1200
Video Resolution (Remote Console)	1280x1024, 1024x768, 800x600, 640x480, 720x400
High Color Depth	16 bits
Remote Control	KVM Console (Java Applet), Terminal Console
Serial Port Mode	Configuration Console (load setup default) Serial over LAN (passthrough access to serial port), Power Control
IP Settings	DHCP, Fixed IP, DDNS
Network Connection	10/100 BaseT
Protocols	TCP, IP, ARP, ICMP, HTTP/HTTPS, SSH, DHCP, NTP, DNS and Dynamic DNS
Management Interface	Web
Security	SSL 256-bit data encryption Secure encryption of keyboard and mouse signals Inactivity timeout
Authentication	SSL Certificate
Firmware Upgrade	via Web interface

Appendix B: Creating CA Files

You need to install openssl toolkit before create the CA files mentioned above. We explain here how to generate the certificate for the IP KVM web server using openssl. You can refer to http://www.openssl.org. for more details about OpenSSL.

Download OpenSSL

1. Download OpenSSL from http://www.slproweb.com/products/Win32OpenSSL.html.
2. Here we are using **Win32OpenSSL_Light-0_9_8j.exe** for the example.
3. Double click on the file to install **Win32OpenSSL_Light-0_9_8j.exe**.
   If you have problem to install the software, please install **Microsoft Visual C++ 2008 Redistributable Package(x86)** from Microsoft website http://www.microsoft.com/downloads/details.aspx?familyid=9B2DA534-3E03-4391-8A4D-074B9F2BC1BF&displaylang=en.

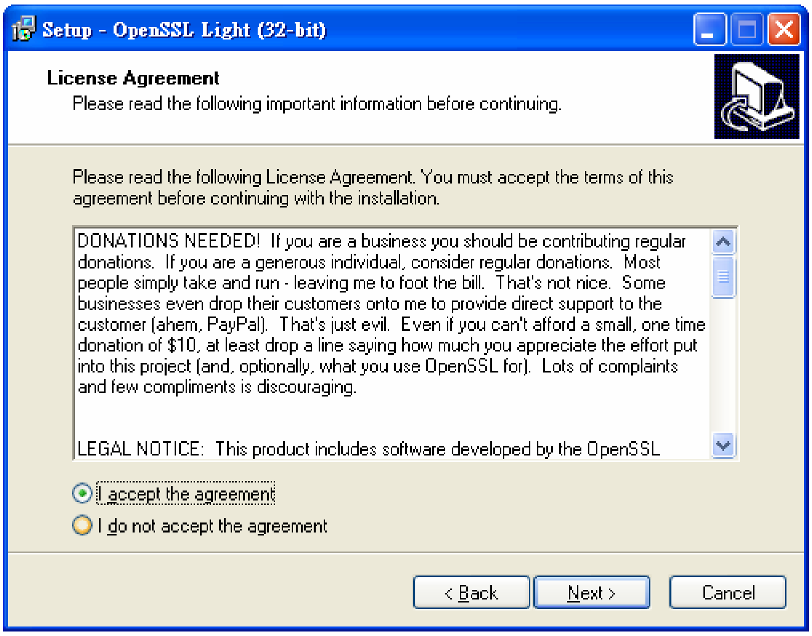


Welcome to the OpenSSL Light (32-bit) Setup Wizard

This will install OpenSSL 0.9.8k Light (32-bit) on your computer.

It is recommended that you close all other applications before continuing.

Click Next to continue, or Cancel to exit Setup.



License Agreement

Please read the following important information before continuing.

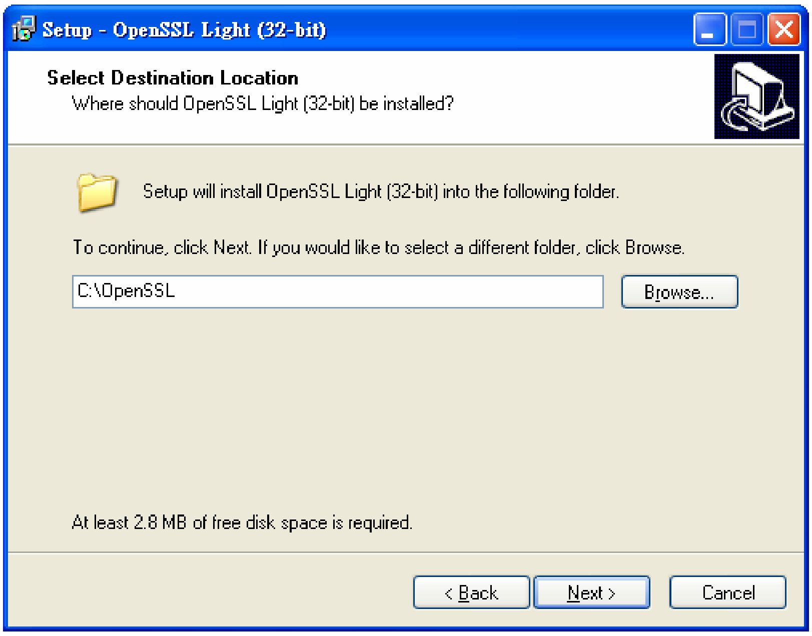
Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.

DONATIONS NEEDED! If you are a business you should be contributing regular donations. If you are a generous individual, consider regular donations. Most people simply take and run - leaving me to foot the bill. That's not nice. Some businesses even drop their customers onto me to provide direct support to the customer (ahem, PayPal). That's just evil. Even if you can't afford a small, one time donation of $10, at least drop a line saying how much you appreciate the effort put into this project (and, optionally, what you use OpenSSL for). Lots of complaints and few compliments is discouraging.

LEGAL NOTICE: This product includes software developed by the OpenSSL

● I accept the agreement

○ I do not accept the agreement



Select Destination Location

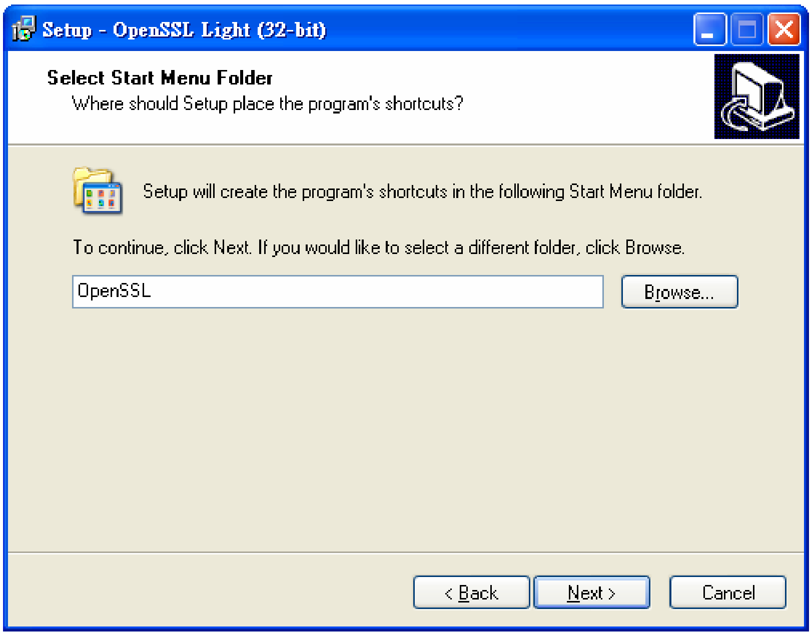
Where should OpenSSL Light (32-bit) be installed?

Setup will install OpenSSL Light (32-bit) into the following folder.

To continue, click Next. If you would like to select a different folder, click Browse.

C:\OpenSSL

At least 2.8 MB of free disk space is required.



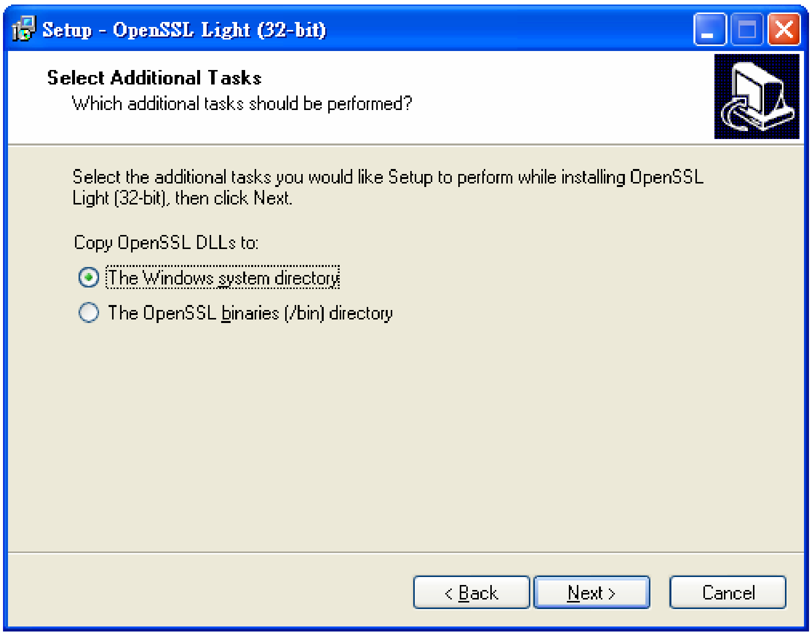
Select Start Menu Folder

Where should Setup place the program's shortcuts?

Setup will create the program's shortcuts in the following Start Menu folder.

To continue, click Next. If you would like to select a different folder, click Browse.

OpenSSL



Select Additional Tasks

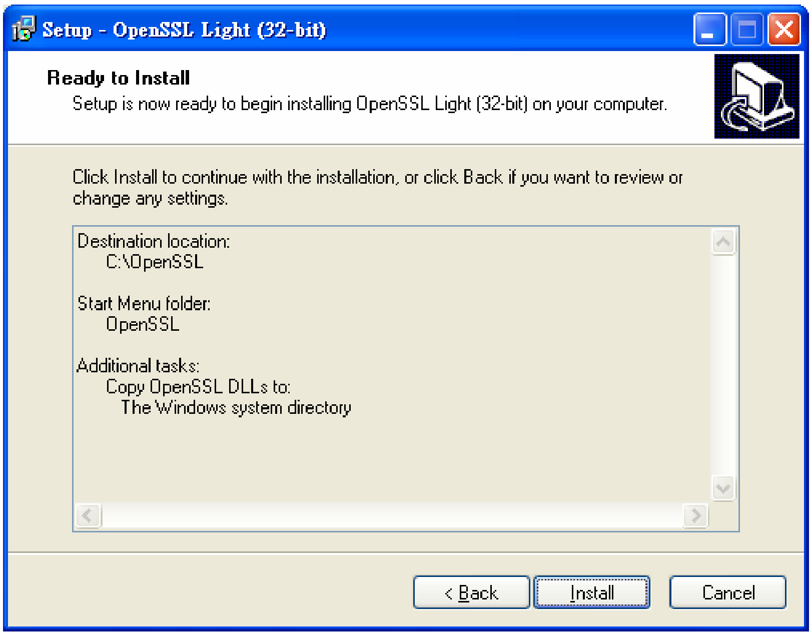
Which additional tasks should be performed?

Select the additional tasks you would like Setup to perform while installing OpenSSL Light (32-bit), then click Next.

Copy OpenSSL DLLs to:

● The Windows system directory

○ The OpenSSL binaries (/bin) directory

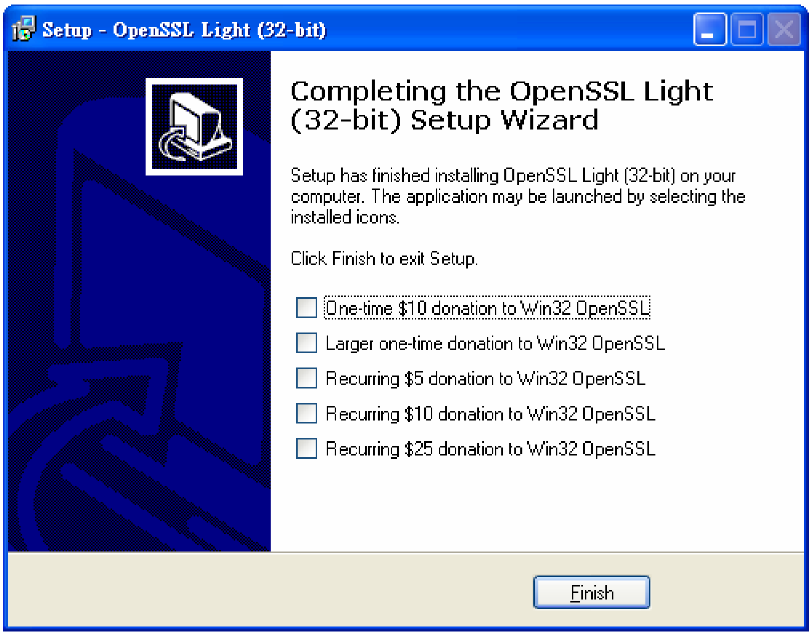


Ready to Install

Setup is now ready to begin installing OpenSSL Light (32-bit) on your computer.

Click Install to continue with the installation, or click Back if you want to review or change any settings.

```
Destination location:
    C:\OpenSSL

Start Menu folder:
    OpenSSL

Additional tasks:
    Copy OpenSSL DLLs to:
      The Windows system directory
```



Completing the OpenSSL Light (32-bit) Setup Wizard

Setup has finished installing OpenSSL Light (32-bit) on your computer. The application may be launched by selecting the installed icons.

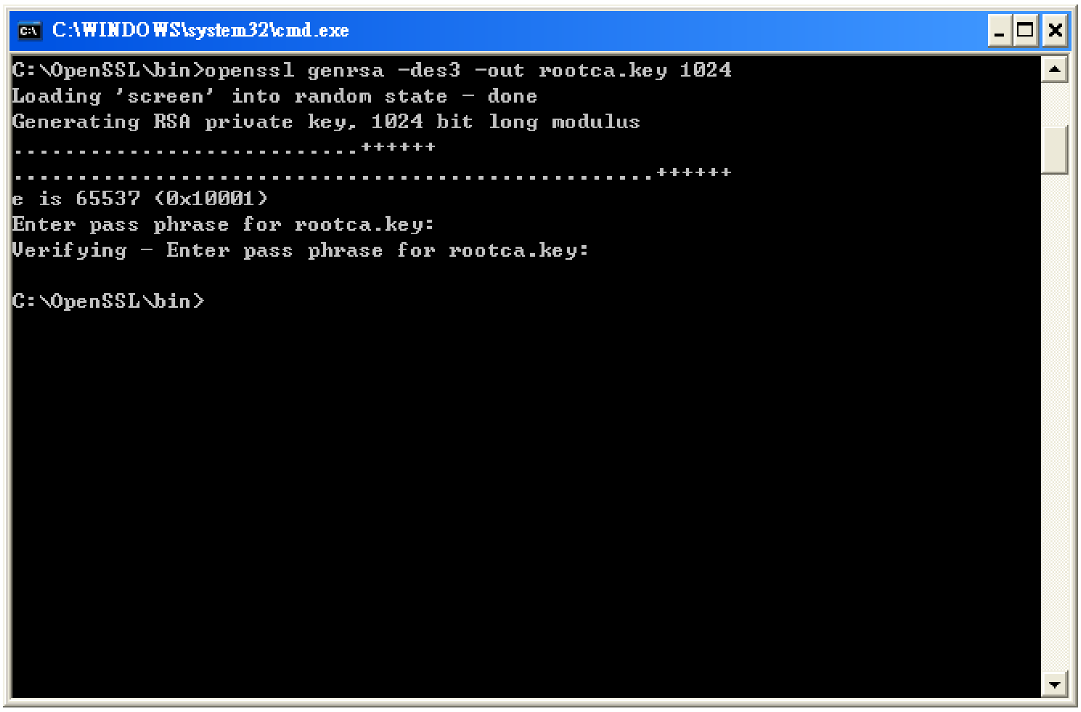
Click Finish to exit Setup.

- □ One-time $10 donation to Win32 OpenSSL
- □ Larger one-time donation to Win32 OpenSSL
- □ Recurring $5 donation to Win32 OpenSSL
- □ Recurring $10 donation to Win32 OpenSSL
- □ Recurring $25 donation to Win32 OpenSSL

4. If you have problem to run the software after installation. Please install **Microsoft Visual C++ 2008 Redistributable Package(x86)** from Microsoft website http://www.microsoft.com/downloads/details.aspx?familyid=9B2DA534-3E03-4391-8A4D-074B9F2BC1BF&displaylang=en.

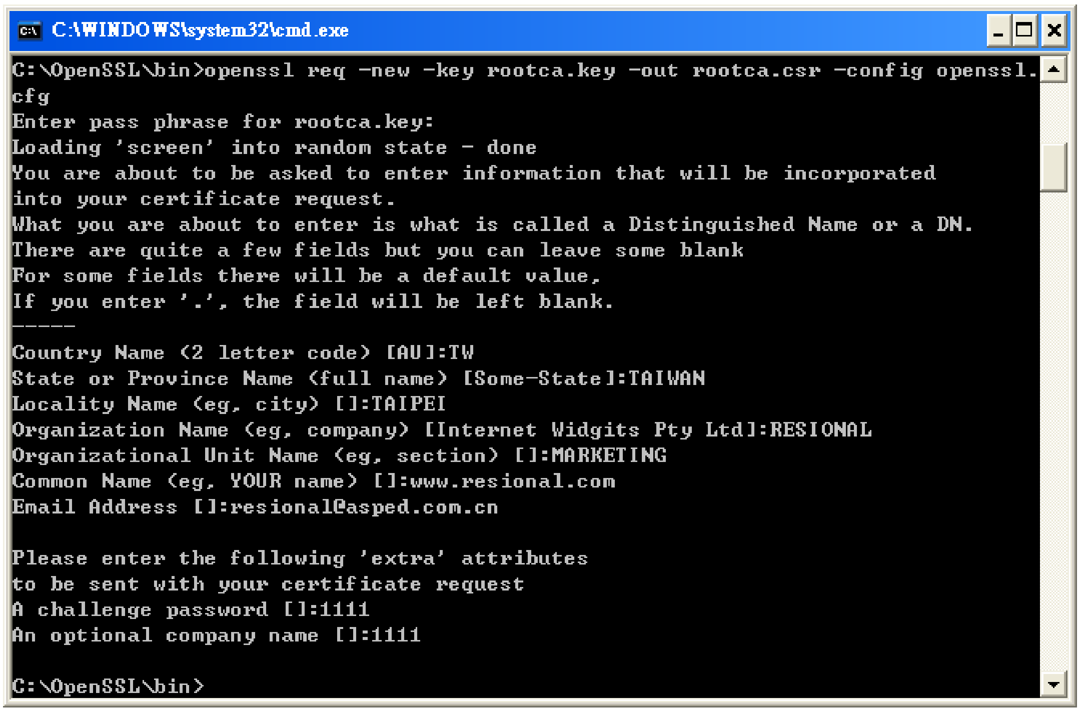
Create Certificate

1. Prepare for RootCA key.
   openssl genrsa -des3 -out rootca.key 1024



```
C:\OpenSSL\bin>openssl genrsa -des3 -out rootca.key 1024
Loading 'screen' into random state - done
Generating RSA private key, 1024 bit long modulus
..........................++++++
................................................++++++
e is 65537 (0x10001)
Enter pass phrase for rootca.key:
Verifying - Enter pass phrase for rootca.key:

C:\OpenSSL\bin>
```

2. Create RootCA Certificate Signing Request (CSR).
   openssl req -new -key rootca.key -out rootca.csr –config openssl.cfg



```
C:\OpenSSL\bin>openssl req -new -key rootca.key -out rootca.csr -config openssl.
cfg
Enter pass phrase for rootca.key:
Loading 'screen' into random state - done
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:TW
State or Province Name (full name) [Some-State]:TAIWAN
Locality Name (eg, city) []:TAIPEI
Organization Name (eg, company) [Internet Widgits Pty Ltd]:RESIONAL
Organizational Unit Name (eg, section) []:MARKETING
Common Name (eg, YOUR name) []:www.resional.com
Email Address []:resional@asped.com.cn

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:1111
An optional company name []:1111

C:\OpenSSL\bin>
```

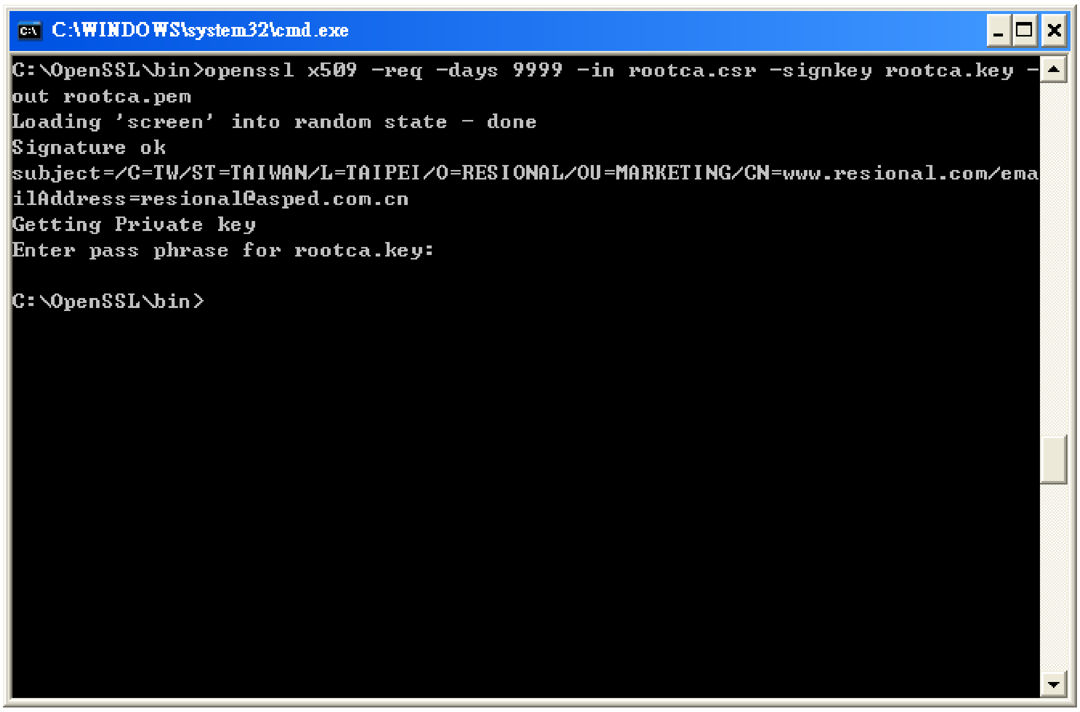
You will be prompted for the PEM pass phrase twice for the key and than you have to enter some information necessary for the certificate:

Here is an example:

Country Name	CHINA
State or Province Name	GUANGDONG
City or Locality	DONGGUAN
Organization Name	ANNSO
Prolix Organizational Unit	MARKETING
Common Name (SERVER HOST NAME)	www.annso.com
Server Administrator's Email Address	sales@annso.com.cn

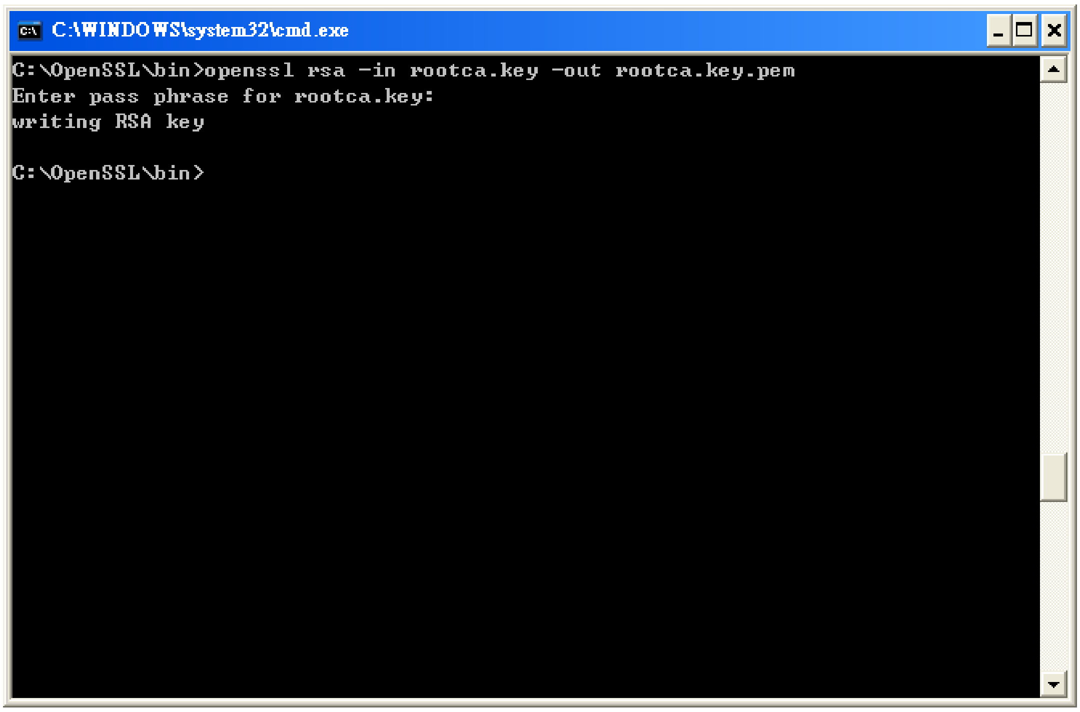
Note: You need to have a DNS server to resolve the Domain name (Common Name), otherwise, please just enter the IP address.

3. Signed by Trustworthy CA.
   openssl x509 -req -days 9999 -in rootca.csr -signkey rootca.key –out rootca.pem



```
C:\OpenSSL\bin>openssl x509 -req -days 9999 -in rootca.csr -signkey rootca.key -
out rootca.pem
Loading 'screen' into random state - done
Signature ok
subject=/C=TW/ST=TAIWAN/L=TAIPEI/O=RESIONAL/OU=MARKETING/CN=www.resional.com/ema
ilAddress=resional@asped.com.cn
Getting Private key
Enter pass phrase for rootca.key:

C:\OpenSSL\bin>
```

4. Remove the passphrase of Rootkey.
   openssl rsa -in rootca.key -out rootca.key



```
C:\OpenSSL\bin>openssl rsa -in rootca.key -out rootca.key.pem
Enter pass phrase for rootca.key:
writing RSA key

C:\OpenSSL\bin>
```

You can now upload the CA files to your IP KVM from **Configuration→SSL Certificate** page.

Appendix C: Certifications

FCC

This equipment has been tested and found to comply with Part 15 of the FCC Rules. Operation is subject to the following two conditions:
(1) This device may not cause harmful interference, and
(2) This device must accept any interference received, including interference that may cause undesired operation.

CE Mark Warning

This equipment is in compliance with the requirements of the following regulations:
EN 55 022: Class B.

RoHS

All contents of this package, including products, packing materials and documentation comply with RoHS.